

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Masatoshi SAKURAI, et al.

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: RECORDING MEDIUM, RECORDING-MEDIUM MANAGEMENT METHOD, AND RECORDING-MEDIUM MANAGEMENT SYSTEM

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed

☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2002-190264	June 28, 2002

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)
☐ are submitted herewith
☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.


Marvin J. Spivak

Registration No. 24,913

C. Irvin McClelland
Registration Number 21,124



22850

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 6月28日

出 願 番 号

Application Number:

特願2002-190264

[ST.10/C]:

[JP2002-190264]

出 願 人

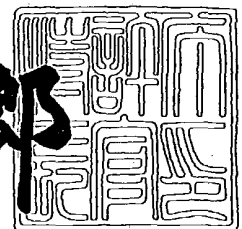
Applicant(s):

株式会社東芝

2003年 4月11日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田 信一郎



【書類名】 特許願

【整理番号】 PTS0173

【提出日】 平成14年 6月28日

【あて先】 特許庁長官殿

【国際特許分類】 G11B 5/00

【発明の名称】 記録媒体、認証方法、認証システム及び復元システム

【請求項の数】 16

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝
研究開発センター内

 【氏名】 櫻井 正敏

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝
研究開発センター内

 【氏名】 鎌田 芳幸

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝
研究開発センター内

 【氏名】 内藤 勝之

【特許出願人】

 【識別番号】 000003078

 【氏名又は名称】 株式会社 東芝

【代理人】

 【識別番号】 100088487

 【弁理士】

 【氏名又は名称】 松山 允之

【選任した代理人】

 【識別番号】 100108062

 【弁理士】

【氏名又は名称】 日向寺 雅彦

【手数料の表示】

【予納台帳番号】 087469

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プールの要否】 要

【書類名】 明細書

【発明の名称】 記録媒体、認証方法、認証システム及び復元システム

【特許請求の範囲】

【請求項 1】

第 1 の書き込み条件によりデータの書き換えが少なくとも一回可能な RAM ビットと、前記第 1 の書き込み条件ではデータの書き換えが不可能な ROM ビットと、が配列してなる認証領域と、

データを格納するデータ格納領域と、
を備えたことを特徴とする記録媒体。

【請求項 2】

前記 RAM ビット及び ROM ビットのそれぞれは、前記第 1 の書き込み条件ではデータの書き込みが不可能な非記録領域により取り囲まれてなることを特徴とする請求項 1 記載の記録媒体。

【請求項 3】

第 1 の書き込み条件によりデータの書き換えが少なくとも一回可能な RAM ビットと、前記第 1 の書き込み条件ではデータの書き換えが不可能な ROM ビットと、が配列してなる認証領域における前記 RAM ビット及び ROM ビットのデータを読み出してその配列に基づいた第 1 のデータ列を取得し、

前記 RAM ビットに任意のデータを上書きし、

前記 RAM ビット及び ROM ビットのデータを読み出してその配列に基づいた第 2 のデータ列を取得し、

暗号化されたデータの復号化処理を、前記第 1 及び第 2 のデータ列に基づいて実行する、

ことを特徴とする認証方法。

【請求項 4】

第 1 の書き込み条件によりデータの書き換えが少なくとも一回可能な RAM ビットと、前記第 1 の書き込み条件ではデータの書き換えが不可能な ROM ビットと、が配列してなる認証領域における前記 RAM ビット及び ROM ビットのデータを読み出してその配列に基づいた第 1 のデータ列を取得し、

前記RAMビットに任意のデータを上書きし、

前記RAMビット及びROMビットのデータを読み出してその配列に基づいた第2のデータ列を取得し、

前記第1及び第2のデータ列に基づいて、任意の処理に関する可否判定を行う

ことを特徴とする認証方法。

【請求項5】

第1の書き込み条件によりデータの書き換えが少なくとも一回可能なRAMビットと、前記第1の書き込み条件ではデータの書き換えが不可能なROMビットと、が配列してなる認証領域を有する記録媒体に関する認証を実行する認証システムであって、

前記RAMビット及びROMビットのデータを読み出してその配列に基づいた第1のデータ列を取得し、

前記RAMビットに任意のデータを上書きし、

前記RAMビット及びROMビットのデータを読み出してその配列に基づいた第2のデータ列を取得し、

前記記録媒体に関する認証を、前記第1及び第2のデータ列に基づいて実行する、

ことを特徴とする認証システム。

【請求項6】

前記認証は、前記記録媒体に暗号化されて格納されたデータの復号化処理であることを特徴とする請求項5記載の認証システム。

【請求項7】

前記認証は、前記記録媒体に格納されたデータに対するアクセスの可否判定であることを特徴とする請求項5記載の認証システム。

【請求項8】

前記上書きする前記任意のデータは、異なる2値のうちのいずれか一方のみからなることを特徴とする請求項5～7のいずれか1つに記載の認証システム。

【請求項9】

前記上書きする前記任意のデータは、前記RAMビットと前記ROMビットの前記配列に対応して、異なる2値のうちのいずれか一方と他方とが交互に出現するものであることを特徴とする請求項5～7のいずれか1つに記載の認証システム。

【請求項10】

前記記録媒体は、複数の前記認証領域を有し、

前記複数の認証領域のそれぞれに対応して、前記第1のデータ列を取得し、前記任意のデータを上書きし、前記第2のデータ列を取得し、前記認証を実行することを特徴とする請求項5～9のいずれか1つに記載の認証システム。

【請求項11】

第1の書き込み条件によりデータの書き換えが可能なRAMビットと、前記第1の書き込み条件ではデータの書き換えが不可能なROMビットと、が配列してなる認証領域を有する記録媒体に関する認証処理が実行された後に、その記録媒体に対して復元処理を実行する復元システムであって、

前記認証処理として、

前記RAMビット及びROMビットのデータを読み出してその配列に基づいた第1のデータ列を取得し、

前記RAMビットに任意のデータを上書きし、

前記RAMビット及びROMビットのデータを読み出してその配列に基づいた第2のデータ列を取得し、

前記記録媒体に格納されたデータに関する認証が、前記第1及び第2のデータ列に基づいて実行され、

前記復元処理として、前記記録媒体に対して前記認証処理が実行された場合に前記第1のデータ列が得られるように、前記RAMビットにデータを上書きすることを特徴とする復元システム。

【請求項12】

前記認証システムは、取得した前記第1及び第2のデータ列の少なくとも一つを記憶しておくメモリーを具備し、当該メモリーに記憶された前記第1及び第2のデータ列の少なくとも一つを消去する機能を具備していることを特徴とする請

求項5～10のいずれか1つに記載の認証システム。

【請求項13】

前記メモリーに記憶された第1及び第2のデータ列の少なくとも一つの消去は、当該データ列に対応するデータ領域の読み出しを一定回数全て終了した場合に行われることを特徴とする請求項12に記載の認証システム

【請求項14】

前記メモリーに記憶された第1及び第2のデータ列の少なくとも一つの消去は、当該データ列に対応するデータ領域を含む記録媒体を認証システムを含む再生装置から外部に取り出した場合に行われることを特徴とする請求項12に記載の認証システム

【請求項15】

前記メモリーに記憶された第1及び第2のデータ列の少なくとも一つの消去は、当該データ列を取得した時点から一定時間終了した場合に行われることを特徴とする請求項12に記載の認証システム

【請求項16】

前記メモリーに記憶された第1及び第2のデータ列の少なくとも一つの消去は、認証システムの使用を終了した場合に行われることを特徴とする請求項12に記載の認証システム

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、記録媒体、認証方法、認証システム及び復元システムに関し、例えば、記録媒体に格納されたコンテンツの復号化やアクセスの可否などを管理するための記録媒体、この記録媒体を用いた認証方法この認証方法を実行可能な認証システム、及びこの記録媒体を復元するための復元システムに関する。

【0002】

【従来の技術】

デジタルデータの普及に伴い、音楽ソフトやビデオソフト、アプリケーションソフト等の著作権保護のためのコピープロテクション技術の重要性が増している

。コピープロテクトが特に要求されるソフトウェアの代表例としては、デジタル記録方式を採用したDVD (Digital Versatile Disk) ビデオディスクあるいはDVD-ROMディスクなどを挙げることができる。これらデジタル記録のビデオソフトウェアに対するコピープロテクションには、従来、暗号化技術が利用されている。

【0003】

暗号化技術を用いたコピープロテクト方法は、既に暗号化されたデータが記録されるDVDビデオディスクあるいはDVD-ROMディスクについては、有効に機能している。しかし、ユーザが新規にデータを記録できるDVD-RAMの場合、次のような問題が生じる。

【0004】

(1) 暗号化の際に必要とされる「暗号鍵」の管理が難しい。

【0005】

(2) ユーザの手元に渡ってしまうデータ記録再生装置（例えば、広く普及しているアナログビデオカセットレコーダと同様に録画・再生をデジタルで行えるDVD-RAMレコーダなど）では強力な暗号化処理が難しく、暗号が破られてしまいやすい。

【0006】

(3) データ記録再生装置側で暗号化およびその復号化が行えるようになっている場合、一旦ユーザが作成して暗号化したデータを別のデータ記録再生装置で復号化した後で再度暗号化する処理を行うことにより、コピープロテクトしたいデータ内容のコピーが容易に行われてしまう。

【0007】

これらの問題のために、デジタルビデオデータの記録再生装置に関しては、従来の暗号化技術を用いたコピープロテクトを有効に機能させることが難しい。また、DVD-RAMドライブ側でDVD-RAM用データ記録媒体に対して独自の 방법으로コピープロテクト処理を行おうとすると、そのデータ記録媒体をDVD-ROMドライブで再生したり、逆にDVD-ROMディスクをDVD-RAMドライブで再生する場合に、コピープロテクト処理回路が複雑になるという問題

がある。このことはまた、DVD-RAMドライブの製品コストをアップさせる要因ともなる。

【0008】

【発明が解決しようとする課題】

本発明は、かかる課題の認識に基づいてなされたものであり、その目的は、記録データに対する安全かつ確実なコピープロテクトを行うことができ、不正コピーを防止できる記録媒体、認証方法、認証システム及び復元システムを提供することにある。

【課題を解決するための手段】

上記目的を達成するため、本発明の記録媒体は、第1の書き込み条件によりデータの書き換えが少なくとも一回可能なRAMビットと、前記第1の書き込み条件ではデータの書き換えが不可能なROMビットと、が配列してなる認証領域と

データを格納するデータ格納領域と、を備えたことを特徴とする。

【0009】

上記構成によれば、記録データに対する安全かつ確実なコピープロテクトを行うことができ、不正コピーを防止できる。

【0010】

なお、本願明細書において、「データの書き換えが少なくとも一回可能なRAMビット」とは、何回でもデータの書き換えが可能なもののみならず、いわゆる「ライトワンス」すなわち一回のみ書き換えが可能なもののよう、データの書込回数が制限されているようなものも含むものとする。

【0011】

上記記録媒体において、前記RAMビット及びROMビットのそれぞれは、前記第1の書き込み条件ではデータの書き込みが不可能な非記録領域により取り囲まれてなるものとすることができる。

【0012】

一方、本発明の第1の認証方法は、第1の書き込み条件によりデータの書き換えが少なくとも一回可能なRAMビットと、前記第1の書き込み条件ではデータ

の書き換えが不可能なROMビットと、が配列してなる認証領域における前記RAMビット及びROMビットのデータを読み出してその配列に基づいた第1のデータ列を取得し、

前記RAMビットに任意のデータを上書きし、

前記RAMビット及びROMビットのデータを読み出してその配列に基づいた第2のデータ列を取得し、

暗号化されたデータの復号化処理を、前記第1及び第2のデータ列に基づいて実行する、ことを特徴とする。

【0013】

上記構成によれば、記録データに対する安全かつ確実なコピープロテクトを行うことができ、不正コピーを防止できる。

【0014】

また、本発明の第2の認証方法は、第1の書き込み条件によりデータの書き換えが少なくとも一回可能なRAMビットと、前記第1の書き込み条件ではデータの書き換えが不可能なROMビットと、が配列してなる認証領域における前記RAMビット及びROMビットのデータを読み出してその配列に基づいた第1のデータ列を取得し、

前記RAMビットに任意のデータを上書きし、

前記RAMビット及びROMビットのデータを読み出してその配列に基づいた第2のデータ列を取得し、

前記第1及び第2のデータ列に基づいて、任意の処理に関する可否判定を行う、ことを特徴とする。

【0015】

上記構成によっても、記録データに対する安全かつ確実なコピープロテクトを行うことができ、不正コピーを防止できる。

【0016】

一方、本発明の認証システムは、第1の書き込み条件によりデータの書き換えが少なくとも一回可能なRAMビットと、前記第1の書き込み条件ではデータの書き換えが不可能なROMビットと、が配列してなる認証領域を有する記録媒体

に関する認証を実行する認証システムであって、

前記RAMビット及びROMビットのデータを読み出してその配列に基づいた第1のデータ列を取得し、

前記RAMビットに任意のデータを上書きし、

前記RAMビット及びROMビットのデータを読み出してその配列に基づいた第2のデータ列を取得し、

前記記録媒体に関する認証を、前記第1及び第2のデータ列に基づいて実行する、ことを特徴とする。

【0017】

上記構成によれば、記録データに対する安全かつ確実なコピープロテクトを行うことができ、不正コピーを防止できる記録媒体、認証方法、認証システム及び復元システムを提供することにある。

【0018】

ここで、前記認証は、前記記録媒体に暗号化されて格納されたデータの復号化处理であるものとすることができる。

【0019】

または、前記認証は、前記記録媒体に格納されたデータに対するアクセスの可否判定であるものとすることができる。

【0020】

また、前記上書きする前記任意のデータは、異なる2値のうちのいずれか一方のみからなるものとすることができる。

【0021】

また、前記上書きする前記任意のデータは、前記RAMビットと前記ROMビットの前記配列に対応して、異なる2値のうちのいずれか一方と他方とが交互に出現するものであるものとすることができる。

【0022】

また、前記記録媒体は、複数の前記認証領域を有し、前記複数の認証領域のそれぞれに対応して、前記第1のデータ列を取得し、前記任意のデータを上書きし、前記第2のデータ列を取得し、前記認証を実行するものとすることができる。

【 0 0 2 3 】

一方、本発明の復元システムは、第 1 の書き込み条件によりデータの書き換えが可能な RAM ビットと、前記第 1 の書き込み条件ではデータの書き換えが不可能な ROM ビットと、が配列してなる認証領域を有する記録媒体に関する認証処理が実行された後に、その記録媒体に対して復元処理を実行する復元システムであって、

前記認証処理として、

前記 RAM ビット及び ROM ビットのデータを読み出してその配列に基づいた第 1 のデータ列を取得し、

前記 RAM ビットに任意のデータを上書きし、

前記 RAM ビット及び ROM ビットのデータを読み出してその配列に基づいた第 2 のデータ列を取得し、

前記記録媒体に格納されたデータに関する認証が、前記第 1 及び第 2 のデータ列に基づいて実行され、

前記復元処理として、前記記録媒体に対して前記認証処理が実行された場合に前記第 1 のデータ列が得られるように、前記 RAM ビットにデータを上書きすることを特徴とする。

【 0 0 2 4 】

一方、上記認証システムにおいて、前記認証システムは、取得した前記第 1 及び第 2 のデータ列の少なくとも一つを記憶しておくメモリーを具備し、当該メモリーに記憶された前記第 1 及び第 2 のデータ列の少なくとも一つを消去する機能を具備しているものとすることができる。

【 0 0 2 5 】

また、前記メモリーに記憶された第 1 及び第 2 のデータ列の少なくとも一つの消去は、当該データ列に対応するデータ領域の読み出しを一定回数全て終了した場合に行われるものとすることができる。

【 0 0 2 6 】

また、前記メモリーに記憶された第 1 及び第 2 のデータ列の少なくとも一つの消去は、当該データ列に対応するデータ領域を含む記録媒体を認証システムを含

む再生装置から外部に取り出した場合に行われるものとすることができる。

【0027】

また、前記メモリーに記憶された第1及び第2のデータ列の少なくとも一つの消去は、当該データ列を取得した時点から一定時間終了した場合に行われるものとすることができる。

【0028】

また、前記メモリーに記憶された第1及び第2のデータ列の少なくとも一つの消去は、認証システムの使用を終了した場合に行われるものとすることができる。

【発明の実施の形態】

以下、具体例を参照しつつ本発明の実施の形態について説明する。

【0029】

(第1の実施例)

まず、本発明の実施の形態にかかる記録媒体およびそれを用いた認証方法の具体例について説明する。

【0030】

図1は、本発明の実施の形態にかかる記録媒体の一例を表す模式図である。すなわち、同図(a)に表したものは、ディスク状の記録媒体であり、例えば、ハードディスクやその他の磁気ディスク、DVD、CDなどの各種の光ディスク、あるいはMO (Magneto-optical) ディスクなどの光磁気ディスクなどの各種の記録方式のいずれかを用いたものである。但し、本発明の記録媒体は、ディスク状のものには限定されず、後に詳述するように、カード状、テープ状、フィルム状など、各種のものを用いることができる。さらに、いわゆる半導体メモリを備えた記録媒体にまで本発明を適用することも可能である。

【0031】

さて、図1に表したように、本発明の記録媒体10Aには、認証領域20が設けられている。図1においては、ディスク状の媒体の中心付近にひとつの認証領域20が設けられている具体例を表したが、後に詳述するように、認証領域20の位置やその数についても、用途に応じて適宜決定することができる。

【0032】

記録媒体10Aにおいて、認証領域20以外の部分はデータ格納領域30であり、例えば、データの読み出しのみが可能な、いわゆるROM (read only memory) 領域とすることができる。但し、このデータ格納領域30を、データの書き込み・読み出しが自在に可能な、いわゆるRAM (random access memory) 領域としてもよく、一度だけデータの書き込みが可能な、いわゆるライトワンス領域 (write once memory) としてもよく、あるいは、ROM領域とRAM領域とライトワンス領域のいずれかを組み合わせたものとしてもよい。

【0033】

そして、後に詳述するように、本発明のひとつの実施の形態においては、このデータ格納領域30に格納されたデータは、暗号化されている。そして、この暗号化されたデータを復号化処理するための「暗号鍵」が、認証領域20に格納されている。

【0034】

また、本発明の別の実施の形態においては、データ格納領域30に格納されたデータに対するアクセス、あるいはこのデータに関する実行処理、演算処理、インストール処理などの各種の処理についての可否判断を、認証領域20に格納されたデータに基づいて行う。つまり、認証領域20において取得されたデータが、所定の内容でない場合には、例えば、アプリケーション・ソフトウェアの実行やインストール、コピーなどが禁止される。

【0035】

図1(b)は、認証領域20の一部拡大図である。本発明の認証領域20は、非記録領域22の中に、RAMビット24と、ROMビット26とが適宜設けられた構造を有する。ここで、非記録領域22は、記録再生ヘッド200によって情報記録を行わない領域である。この非記録領域は、情報を記録することが不可能な材料によって構成されていることが好ましいが、情報を記録することが可能な材料で構成されていてもよい。

【0036】

そして、同図において、RAMビット24は、記録再生ヘッドなどにより情報

の記録が可能な最小単位とする。すなわち、RAMビット24は、記録再生ヘッドなどにより、これらビットへの記録を行うことで、情報を書き換えることが可能なビットである。

【0037】

RAMビット24の具体的な材料は、例えば、情報を磁気的に書き込むことができる磁性体や、結晶-非晶質転移により光反射率が変化する相変化媒体、その他、電場、光照射、加熱、酸化還元反応などにより、色の変化する各種クロミック材料や形状の変化する材料、導電率、誘電率、光透過率などが変化する材料など、何らかの手法で情報を書き換えることができる材料で構成されているならば何でもよい。またさらに、半導体RAMメモリのように、電荷を蓄積することにより情報の書き換えが可能なものでもよい。

【0038】

一方、ROMビット26は、情報の書き換えが不可能であるか、または、RAMビット24と異なる方法によらなければ情報の書き換えができない領域である。但し、このROMビット26も、記録再生ヘッドなどによってRAMビット24と同様に情報が読み取り可能なビットである。すなわち、「0」や「1」、もしくは直前のRAMビットもしくはROMビットの情報と同じ情報などを与える領域である。

【0039】

RAMビット24とROMビット26は、本発明における認証領域20内において、例えば、記録再生装置の読み取りクロック周波数に応じたある一定間隔で配列している。但し、その間隔は、適用する記録再生システムに応じて適宜決定することができ、必ずしも一定の間隔である必要はない。

【0040】

そして、本発明においては、1つの認証領域20内に、RAMビット24とROMビット26が少なくとも一つずつ以上設けられる。これらRAMビット24とROMビット26の数や配列の順序は、用途に応じて適宜決定することができる。また、その配列に関しては、図1に例示したように一次元的に並べるものには限定されず、所定の面内に2次元的に並べてもよく、またさらに、多層記録媒

体などの場合には、3次元的に並べることも可能である。

【0041】

但し、認証領域20におけるRAMビット24とROMビット26の配列パターンは、予測不可能なものが好ましい。すなわち、認証領域20におけるRAMビットとROMビットの配置は、そのビットがRAMビットであるかROMビットであるかで変わるものではなく、両方のビット共に一定の規則で配列されていることが好ましい。これによって認証領域20中の各ビットを再生ヘッドや記録ヘッドでアクセスしただけでは、そのビットがROMビットであるかRAMビットであるかが判別困難であるものが好ましい。さらに、例えば記録媒体毎に異なるパターンであるとか、複数のパターンをディスク毎にランダムに用いて、予測困難にすることが望ましい。そうすることによって、後に詳述するように、「鍵B」の予測が困難になり、コピープロテクトの信頼性が高くなるからである。

【0042】

以下、このような記録媒体を用いて実行可能な認証プロセスについて説明する。

【0043】

図2は、本発明による認証方法を説明する概念図である。

【0044】

すなわち、本発明の認証方法は、「鍵A取得」「上書きイレース」「鍵B取得」という一連の認証プロセスからなる。

【0045】

なお、本具体例においては、ROMビット26の全てが、「0」や「1」など特定のビット情報として記録再生ヘッド200により読みとり可能な場合を例に挙げる。図2(a)～(c)のそれぞれにおいては、各ステップにおける認証領域20の状態を表した。ここで、非記録領域22は、記録再生ヘッド200によって情報を記録することが不可能な領域とする。

【0046】

図2においては、便宜的に、「0」が書き込まれたRAMビット24Aを白丸により表し、「1」が書き込まれたRAMビット24Bを黒丸により表した。こ

これらのRAMビット24A、24Bは、記録再生ヘッド200が再びこれらビットへの記録を行うことで、情報を書き換えることが可能である。

【0047】

本発明の認証方法においては、あらかじめ認証領域20に、「鍵A」の取得のための情報が書き込まれている。

【0048】

図2(a)は、本発明における「鍵A」の取得のプロセスを表す。すなわち、認証領域20において、「0」もしくは「1」の書き込まれたRAMビット24(24A、24B)と、ROMビット26とが配列している。この領域を記録再生ヘッド200が読みとる。なお、本具体例においては、ROMビット26は、「0」として読みとられるものとする。ただし、本発明は、これに限定されるものではない。

【0049】

図2(a)において認証領域20を記録再生ヘッド200が読むと、白丸で表したRAMビット24AおよびROMビット26が「0」として読まれ、黒丸で表したRAMビット24Bが「1」と読まれる。つまり、この認証領域20は、「00101001」と読みとられる。これを、「鍵A」として認識する。

【0050】

次に、図2(b)に表したように、「上書きイレース」を行う。すなわち、「鍵A」を取得した後、この認証領域20に対して記録ヘッド200により「11111111」という情報を上書きする。

【0051】

この「上書きイレース」処理により、記録ヘッドが認証領域20中の全てのビットに「1」を表す信号を書き込もうとした結果、認証領域20の上の「0」を表すRAMビット24A(白丸)と「1」を表すRAMビット24B(黒丸)は、全て「1」を表すビット24B(黒丸)に書き換えられる。この時、この認証領域20上のROMビット26の情報は変わらず、図2の具体例では、「0」の記録がされたままである。

【0052】

次に、図2(c)に表したように、「鍵B」を取得する。すなわち、「上書きイレース」後の認証領域20を、再び再生ヘッド200が読みとることにより、「鍵B」に対応するビットデータを取得する。

【0053】

ここで、前述の「上書きイレース」後、この認証領域20におけるRAMビット24は、全て「1」を表すビット24B（黒丸）になっており、一方、「0」を表すROMビット26に変化はない。したがって、「鍵B」として、再生ヘッド200により、「10111011」というビットデータが読みとられ、これを「鍵B」として認識する。

【0054】

本発明においては、以上の手順により読み出された「鍵A」と「鍵B」の両方を用いて、例えば、暗号鍵（暗号キー）を生成することができる。そして、この暗号鍵を使って、例えば、データ格納領域30に記録されている暗号化されたデータの暗号の復号化処理、すなわち解読を行う。「鍵A」および「鍵B」を用いて暗号鍵を生成する方法は、例えば鍵Aと鍵Bを順番につなげて一つの鍵とするなどがあるが、それ以外でも特定のものに限定されず、「鍵A」および「鍵B」から一つの暗号鍵を生成してもよいし、例えば「鍵A」と「鍵B」をビット加算した「鍵C」と、ビット減算した「鍵D」を得るなど、複数の鍵を生成してもよい。

【0055】

暗号解読の手順は、特に限定されないが、例えば、公開鍵を用いるものではRSA方式などを用いることができる。また、秘密鍵を用いるものとしては、DESや、FEAL、MISTY、IDEAなどを用いることができる。

【0056】

公開鍵と秘密鍵とを用いるような暗号処理の場合、本発明では「鍵A」が「鍵B」に比べアクセスが容易であるため、「鍵A」を公開鍵とし、「鍵B」を秘密鍵として用いることが好ましいが、本発明は、これには限定されない。

【0057】

以上説明した本発明の記録媒体及び認証方法を用いると、強力なコピープロテ

クトが可能となる。

【0058】

すなわち、本発明において、認証領域20は、上述のようにRAMビット24とROMビット26との混在で構成されるが、通常の再生ヘッド200がこの領域をアクセスする時には、認証領域20中のビットのどれがRAMビットでどれがROMビットであるかを判別することは困難である。

【0059】

このため、例えば、本発明における認証処理を行う前のオリジナル記録媒体10A（例えば、DVD-ROM）を、別のコピー記録媒体（例えば、DVD-RAM）にコピーした場合、認証領域20も共にコピーされるが、コピーされるのはあくまでこれらRAMビット24とROMビット26に格納されているビット情報のみであり、RAMビット24とROMビット26の配置情報はコピーできない。

【0060】

したがって、コピー記録媒体のうちの、認証領域がコピーされた領域は、全て書き換え可能なRAMビットにより構成されている。

【0061】

このコピーされた認証領域に対して「鍵A」の取得の作業を行うと、オリジナルの記録媒体と同じ鍵Aが取得できる。

【0062】

しかし、それに引き続き、このコピー媒体の認証領域に対して、「上書きイレース」処理を行うと、前述の通りコピー媒体では認証領域内のビットは全てRAMビットであるため、上書きイレースに用いたパターンがそのまま記録される。

【0063】

従って、次に「鍵B」の取得を行った場合、コピー記録媒体上の認証領域に記録されている情報は「上書きイレース」のパターンがそのまま書き込まれているため、上書きイレースパターンが読み出される。一方、オリジナル記録媒体の認証領域は、前述の通りRAMビットとROMビットが混在しているため、上書きイレースを行った場合もROMビットには記録が不可能であるため、上書きイ

ースパターンと鍵Bのパターンは異なるものとなる。

【0064】

つまり、得られる「鍵B」はオリジナル記録媒体とコピー記録媒体で異なるため、オリジナル記録媒体で暗号解読が可能な「鍵B」をコピー記録媒体では得ることができない。このため、コピー記録媒体では、データ格納領域30に格納されたデータの暗号解読ができず、コンテンツを再生することができない。

【0065】

図3は、上述したオリジナル媒体とコピー媒体の違いを表す概念図である。

【0066】

同図においては、オリジナル媒体上の認証領域20における「鍵」の取得は、図2に表した具体例と同じものを表した。すなわち、「鍵A」として「00101001」が取得され、「上書きイレース」では認証領域に「11111111」を書き込み、「鍵Bとして「10111011」が得られる。

【0067】

これに対して、コピーされた媒体上の認証領域では、「鍵A」は、そのままコピーされているので、図3(a)に表したように、「鍵A」として、オリジナル媒体と同じ「00101001」が得られる。

【0068】

次に、図3(b)に表したように、「11111111」パターンで「上書きイレース」を行うと、コピー媒体は全てのビットがRAMビットで構成されているため、認証領域のビットは全てこのパターンで上書きされてしまう。従って、これに続く「鍵B」の取得プロセスにおいて、コピー媒体では上書きイレースのビットパターンがそのまま「鍵B」として取得され、「11111111」が得られる。

【0069】

すなわち、オリジナル媒体では、ROMビット26が設けられているため、「鍵B」は、上書きイレースのパターンとは異なる「10111011」となるが、コピー媒体では上書きイレースパターンと同じ「11111111」であり、正しい「鍵B」が得られない。このため、コピー媒体では、データ格納領域30

に記録された暗号化データの暗号解読が不可能となる。

【0070】

なお、上述の説明においては、「鍵A」と「鍵B」とを用いて、データ格納領域30に格納されている暗号化データの復号化処理を行う具体例を挙げたが、本発明は、この具体例には限定されない。

【0071】

これ以外にも、例えば、「鍵A」と「鍵B」とを用いて、データ格納領域30に格納されているコンテンツの再生動作の可否を決定したり、また、データ格納領域30に格納されているアプリケーションソフトウェアのインストールや実行動作の可否を決定したりしてもよい。

【0072】

この場合には、例えば、「鍵A」と「鍵B」とに対応するデータをデータ格納領域30にも格納しておく。そして、認証手続により、認証領域20において得られた「鍵A」及び「鍵B」と、データ格納領域30に格納されているこれらの対応データとを照合して、両者が一致した場合のみ、データ格納領域30に格納されているコンテンツの再生や、アプリケーション・ソフトウェアの実行あるいはインストールなどが許可されるようにすることができる。

【0073】

(第2の実施例)

次に、認証領域20において、ROMビット26が、その直前のビットのデータと同じビットデータとして読みとられる場合の実施例について説明する。

【0074】

本発明における「上書きイレース」のパターンは、第1実施例に関して説明したように、「0000・・・」や「11111・・・」の如く同じビットデータの連続である必要はなく、本発明を用いる記録再生システムにおいてROMビット26から得られる信号特性に合わせたものとすることができる。

【0075】

例えば、CDやDVDなどに代表される光記録媒体を用いる場合、各ビットからの反射光の強度をそれぞれビット信号として認識する場合が多く、あるしきい

値以上の信号強度なら「1」、しきい値より小さい信号なら「0」とするなどの読み取り方法を用いる。このように、各ビットからの情報を一定のしきい値で認識する場合は、上書きイレース信号は、前例で述べたように「0000・・・」や「1111・・・」などの同じビット信号の連続が有効である。

【0076】

一方、HDD (Hard Disk Drive) などの場合、磁気情報記録媒体の上でのROMビットは、磁気情報を持たない領域とすることができる。この場合、GMR (Giant Magneto Resistance effect: 巨大磁気抵抗効果) ヘッドなど磁気読み取りヘッドの特性上、このようなROMビットからの信号は、直前に読まれたビットからの信号と同じ信号と認識される。例えば、認識領域において、ROMビットの直前のビットが「0」であったならば、ROMビットも「0」と認識される。

【0077】

この場合には「上書きイレース」に用いるパターンとして、前例のような「111・・・」など、同じ信号が連続したパターンは好ましくない。なぜならば、本発明におけるRAMビットとROMビットとが混在した認証領域を「111・・・」の如く同じ信号の連続パターンで上書きイレースした場合、全てのRAMビットは「1」が記録され、ROMビットは直前のビットと同じものが認識されるため、認証領域のどこにROMビットがあっても「鍵B」は上書きイレースパターンと等しい「1111・・・」が得られてしまうからである。

【0078】

このように、ROMビットを、その直前に読まれたビットと同じデータと認識するようなシステムの場合には、上書きイレースに用いるパターンは、「010101・・・」といのように、異なるビットデータが交互に表れるビットデータ列とすることが望ましい。

【0079】

図4は、HDDのようなシステムにおける認証プロセスを例示する概念図である。

【0080】

同図(a)において、「鍵A」の取得時は、認証領域20のROMビット26、すなわち図中の左から3番目と6番目の記録ビットは、その直前のビットと等しいものとして読み出される。つまり、「鍵A」として、「0111000」が得られる。

【0081】

次に、図4(b)に表したように、上書きイレースを「1010101」と「1」と「0」が交互に配列されたビットパターンを用いて行う。

【0082】

すると、図4(c)に表したように、「鍵B」の読み出しに際しては、ROMビット26をその直前のビットと等しいものとして読み出すため、「鍵B」として「1000111」が得られる。

【0083】

このように、「鍵B」が、上書きイレースパターン「1010101」とは異なるビットデータとなるため、この上書きパターンを用いれば、コピー媒体上にコピーされた認識領域からの「鍵B」と区別することができ、コピープロテクトとして有効となる。

【0084】

このように、「上書きイレース」の時に用いる上書きパターンは、RAMビット24及びROMビット26がどのように読み取られるかというシステムの特性に応じて適宜決定することが望ましい。すなわち、上書きパターンを、同じビットデータの連続とするか、あるいは異なるビットデータの組み合わせとするか、適宜選択する。なお、本具体例においては、上書きパターンとして、「11111111」と「1010101」を用いたが、本発明は、これに限定されるものではなく、上書きパターンと「鍵B」とが異なるビットデータとなれば、どのような上書きパターンも用いることができる。

【0085】

(第3の実施例)

次に、本発明の第3の実施例として、複数の認証領域を有する記録媒体を用いた具体例について説明する。

【0086】

すなわち、本発明の認証方法では、その認証方法の過程に含まれる上書きイレースを行った後では、記録媒体上でRAMビットに上書きイレース前にどんな鍵Aの情報が書き込まれていたかを調べることが不可能になる。従って、本発明においては、同じ認証領域を用いた場合、後述する「復元処理」なしには繰り返し認証を行うことが不可能である。つまり、「復元処理」なしでは、ひとつの認証領域を用いた認証作業が一度だけ可能だという特徴を有する。

【0087】

この特徴を利用すると、記録媒体に記録されたコンテンツの参照回数を制限することなどが可能となる。

【0088】

例えば、記録媒体10Aのデータ格納領域30に一本の映画コンテンツが記録されており、この映画コンテンツは暗号化されており、暗号鍵は、「鍵A」と「鍵B」とを用いて生成され、その「鍵A」および「鍵B」は、認証領域20に記録されているとする。

【0089】

この記録媒体10Aの映画コンテンツを再生する場合、前述した手順に従い認証領域20に対して「鍵A」の取得、「上書きイレース」、「鍵B」の取得、という一連の作業を行うことにより、「鍵A」と「鍵B」とが取得され、これらから暗号鍵を得てコンテンツを暗号解読し、コンテンツへのアクセス及び再生が可能となる。

【0090】

しかし、認証プロセスにおいて、「上書きイレース」を行うため、その次に、認証しようとしても、「鍵A」の取得は不可能となる。したがって、一度コンテンツにアクセス済みの媒体は、もう一度認証作業を行いコンテンツにアクセスすることは不可能となり、一度しかコンテンツにアクセスできないという特徴を実現できる。

【0091】

この特徴を利用して、例えば1つのコンテンツに対して複数の認証領域を対応

させておけば、一つの認証領域は後述する再生処理を行うまでは一度しか認証プロセスを実行できないため、その認証領域の数だけコンテンツへのアクセスを可能とするアクセス制限機能を提供することができる。

【0092】

図5は、複数の認証領域を有する記録媒体を例示する概念図である。すなわち、本具体例の記録媒体10Bは、4つの認証領域20A～20Dを有する。

【0093】

例えば、この記録媒体のデータ格納領域30に暗号化された映画コンテンツを格納し、認証領域20A～20Dにそれぞれ、「鍵A」及び「鍵B」を格納すれば、4回認証作業をすることが可能であるため、映画コンテンツを4回再生することが可能となる。

【0094】

この場合、認証領域に格納する「鍵A」と「鍵B」は、4つの認証領域20A～20Dの間で全く同じものとしてもよいし、異なるものとしてもよい。言い換えると、各認証領域におけるRAMビットとROMビットの配置パターン、並びにRAMビットにあらかじめ記録しておく信号は、各認証領域で全く同じものとしてもよいし、異なるものとしてもよい。つまり、「鍵A」と「鍵B」を、認証領域毎に変えてもよく、認証領域毎に同一としてもよい。

【0095】

また、例えば、一つのコンテンツを複数のチャプターに分割し、それぞれのチャプターに、認証領域20A～20Dのいずれかを割り当てることによって、一度にコンテンツの全体にアクセスしなくても、各チャプターを一つずつ、一回ずつ時間をおいてアクセスすることが可能となる。

【0096】

なお、本発明においては、記録媒体に設けられる認証領域の数やその配置についても、図5に限定されず、用途に応じて適宜決定することができる。

【0097】

(第4の実施例)

次に、本発明の第4の実施例として、認証領域を上書きイレースの前の状態に

戻す「復元処理」について説明する。

【0098】

本発明の記録媒体において、認証プロセスを実行した後の認証領域は、図2乃至図4に関して前述したように、上書きイレースされた状態とされている。従って、このままでは、もう一度認証プロセスを繰り返すことはできない。

【0099】

これに対して、認証領域に「鍵A」のデータをもう一度書き込めば、再度の認証プロセスが可能となる。このような「鍵A」の書き込みのプロセスを、「復元処理」と称することとする。

【0100】

記録媒体上での認証領域の位置が分かるような場合（例えば、認証領域が配置されるトラックやセクターなどが決められている場合）には、単純な書き込み処理によって、復元処理を実行することが可能である。

【0101】

一方、記録媒体上で、認証領域の位置が分からないような場合には、RAMビット24とROMビット26の配列を手がかりとして、媒体上で認証領域を探す必要がある。従って、この場合には、記録媒体の上で、RAMビットとROMビットを区別して識別し、しかる後に、認証領域を判定して、そこに所定の「鍵A」のデータを書き込むという処理が可能な記録システムが必要とされる。

【0102】

図6は、復元処理の応用例を表す模式図である。すなわち、同図は、ビデオレンタルショップにおける復元処理を表す。

【0103】

ビデオレンタルショップは、本発明の認証領域を持った記録媒体と、この認証領域を復元可能な復元装置とを有する。

【0104】

一方、ユーザーは、本発明の認証作業を実行可能な再生装置を有する。

【0105】

ビデオレンタルショップでは、復元装置によって認証領域を復元した記録メデ

ィアをユーザーに貸与する。

【0106】

ユーザーは、貸与された記録メディアを、ユーザーの所有する再生装置によって閲覧する際、暗号化されたコンテンツにアクセスするため、認証作業を行う必要がある。そして、認証作業をし、「鍵A」と「鍵B」とから暗号鍵を生成して、コンテンツにアクセスする。

【0107】

認証作業を一度実行すると、その認証作業に用いた認証領域は上書きイレースされ、そのままでは、再度の認証が不可能になる。

【0108】

ユーザーの所有する再生装置が認証時に読みとった鍵は、その再生装置が鍵を記憶している限りその認証領域に対応するデータを何度でも複合化出来るため、本発明の複数認証の禁止に不都合である。従って本発明におけるユーザーの再生装置では、認証領域から読みとった「鍵A」および「鍵B」を保存していた記憶を、消去するシステムを備えていることが必要である。

【0109】

この「鍵A」および「鍵B」の記憶の消去は、ある一定の事象が起きたときに行われるのが好ましい。「鍵A」および「鍵B」を再生装置が忘却するのは、例えば認証領域を備えた記録媒体からのデータ読み取りを全て終えた時点、もしくはその記録媒体が再生装置から取り出されたとき、もしくは認証作業を行った後の一定時間経過後、もしくは再生装置の使用終了時、たとえば停止スイッチや電源OFFスイッチを押した時などがあるが、特にこれらには限らない。

【0110】

ユーザーは、コンテンツ参照後、記録媒体をビデオレンタルショップに返却する。ビデオレンタルショップでは、返却された記録媒体の認証領域を、復元装置によって再び「鍵A」を取得可能な状態に戻すことにより、再びその記録媒体を認証可能な状態にしてユーザーに提供することができる。

【0111】

(第5の実施例)

次に、本発明の第5の実施例として、本発明の記録媒体の作成方法について具体例を挙げて説明する。

【0112】

本発明における認証領域は、RAMビット24とROMビット26とが混在した領域である。この領域を作成する方法として、あらかじめ記録媒体上に所定の間隔でRAMビット配列を作成しておき、その後、特定のRAMビットを破壊もしくは改質することによって書き込み不可能なROMビットに変える方法を挙げることができる。

【0113】

以下、図面を参照しつつ、本実施例の記録媒体の製造方法について説明する。

【0114】

図7は、本実施例における記録媒体の製造方法を表す工程断面図である。

【0115】

まず、同図(a)に表したように、基板111の上に溝構造を形成した。具体的には、2.5インチのガラスディスク基板111の上に、厚さ約30nmのPt反射膜112、マトリックスとなる厚さ約50nmの Al_2O_3 膜113、および厚さ約50nmの SiO_2 膜114を成膜した。そして、 SiO_2 膜114上にレジスト(図示せず)をスピコートした後、ナノ・インプリンティング・リソグラフィー(nano-imprinting lithography)によりレジストを加工し、幅40nmの凸部によって幅400nmのスパイラル形状の溝を規定するようにレジストパターンを形成した。このレジストパターンをマスクとして、 SiO_2 膜114をエッチングし、溝115を転写した。

【0116】

なおここで「ナノインプリンティングリソグラフィー」とは、ナノメートル・サイズの微細な凹凸パターンを高精度に制御された条件のもとで圧接させることにより、その凹凸パターンを被転写体(本実施例の場合は、レジスト)に転写する技術である。

【0117】

次に、図7(b)に表したように、溝領域内にブロックコポリマーを埋め込ん

で微粒子の規則配列構造を形成した。具体的には、ポリスチレン-ポリメチルメタクリレートブロックコポリマー（PSの分子量 $M_w=30000$ 、PMMAの分子量 $M_w=8000$ ）をトルエンに1% w/wの濃度で溶解した溶液を調製した。試料上に、この溶液をスピコートして SiO_2 膜114に転写された溝領域内に、ブロックコポリマー116を埋め込んだ。次に、この試料を真空中において、150℃で30時間アニールして、ブロックコポリマー116を規則配列化させた。この結果、島状のポリメタクリレート粒子117が海状のポリスチレン部分118によって囲まれた構造が形成された。

【0118】

次に、図7(c)に表したように、RAMビット24のための孔構造を形成した。すなわち、ブロックコポリマー116を紫外線で処理した後、水洗してPMMA部117を除去して、孔部を作製した。次に、斜め蒸着法により、この孔部を埋めないようにCr層119を形成した。そして、RIE (Reactive Ion Etching) により Al_2O_3 膜113に達する孔を形成し、さらにArイオンミリングにより Al_2O_3 膜113に孔120を転写し、 Al_2O_3 膜113からなるマトリックスを形成した。

【0119】

次に、図7(d)に表したように、RAMビット24を形成し、表面を平坦化した。すなわち、厚さ約30nmの相変化材料In-Sb-Te121を成膜して孔120に埋め込み、RAMビット24を形成した。その後、表面をCMPにより研磨して平坦化し、全面に SiO_2 を成膜して保護膜122を形成した。

【0120】

図8は、このようにして形成した相変化光記録媒体を近接場光顕微鏡により観察した結果を模式的に表す図である。同図に表したように、幅400nmの記録トラック帯131と幅約40nmの Al_2O_3 膜113からなる分離帯132とが交互に形成されている。1つの記録トラック帯131内でRAMビット24は、六方細密充填構造をなして三角格子を形成している。RAMビット24は、トラック方向に沿ってピッチPをもって周期的に形成されており、記録トラック帯131内には19列のサブトラックが含まれている。記録トラック帯131内で

隣り合うサブトラック上に位置する最近接の2つのRAMビット24はトラック方向に沿って中心間の間隔がサブトラック内のピッチPの1/2だけずれている。

【0121】

以上のように、RAMビット24の集合体を形成したが、ROMビットの形成はRAMビットの一部24をROMビットにすることにより行う。

【0122】

すなわち、図7(e)に表したように、特定のRAMビット24を除去することにより、ROMビット26とした。すなわち、得られた記録媒体上で、所定の領域のRAMビットがトラック上に8個配列した部分を認証領域20とし、この部分の3番目と6番目のRAMビット24のIn-Sb-Teを電子ビーム加熱により、加熱、除去した。除去した部分には、保護膜122を埋め込んでも良いし、非磁性材料や保磁力のより大きな磁性材料等のRAMビット24と異なる材料を選択的に埋め込んだ後、保護膜122を形成しても良い。

【0123】

AFM (Atomic Force Microscopy) によりこの認証領域20を観察したところ、第1、2、4、5、7、8番目のビット部分は他のRAMビットと同じRAMビット24が確認され、第3、6番目のビットは相変化材料が除去されたことによる凹型ビットとしてのROMビット26が確認できた。

【0124】

図9および図10は、本実施例の記録媒体の再生が可能な相変化光記録再生装置の要部を表す概念図である。

【0125】

すなわち、図9は、記録媒体および光記録再生装置のヘッドスライダを示す断面図である。本実施例の記録媒体141は、ガラス基板111上にRAMビット24が規則配列した記録トラック帯を有する記録層および保護層122が形成されている。この記録媒体141は、スピンドルモーター142に装着され、図示しない制御部からの制御信号により回転する。ヘッドスライダ143の先端には、レーザー共振型の光検出読み出しヘッド144、面発振型レーザー書き込みヘ

ッド145が搭載されている。ヘッドスライダ143は2段アクチュエータ（図示せず）によって位置決めされる。

【0126】

図10は、ヘッドスライダに設けられた微小開口の平面構造を示す概略図である。ここで、読み出しヘッド144の微小開口の寸法は縦35nm、幅20nm、書き込みヘッド145の微小開口の寸法は縦20nm、幅20nmである。

【0127】

この記録再生装置は、パターン化された記録媒体141のRAMビット24とROMビット26、及びその他の記録ビットに対して、シーク動作、「鍵A」の取得、上書きイレース、「鍵B」の取得、その他の記録ビットについての記録読み出し、読み出しヘッドのトラッキング、および欠陥領域への書き込みの回避動作を行うことができる。

【0128】

この記録再生装置を用いて、本実施例の記録媒体を、前述した第1実施例の手法により、上書きイレースパターン「11111111」を用いて認証プロセスを実行した結果、「鍵A」及び「鍵B」が取得された。また、この記録媒体をRAM媒体にコピーしたコピー媒体では再生が不可能なことが確認できた。

【0129】

(第6の実施例)

次に、本発明の第6の実施例として、本発明の記録媒体のもうひとつの作成方法について具体例を挙げて説明する。すなわち、本実施例においては、記録媒体上のビットが形成されていない領域において、特定の部分にRAMビット24を特定の配列で作成し、RAMビット24の無い部分をROMビット26とした。

【0130】

図11は、本実施例における記録媒体の製造方法の要部を表す工程断面図である。

【0131】

まず、同図(a)に表したように、基板41上に溝構造を形成した。すなわち、直径2.5インチのガラスディスク基板41上に、厚さ約30nmのPd下地

層と厚さ約50nmの垂直磁気記録材料CoCrPtとを成膜して磁性層42を形成し、さらに磁性層42上に厚さ約50nmのSiO₂膜43を成膜した。そして、SiO₂膜43上にレジスト44をスピンコートした。

【0132】

その後、ナノ・インプリンティング・リソグラフィーによりレジスト44を加工し、幅40nmの凸部によって幅約400nmのスパイラル形状の溝45を規定するようにレジストパターンを形成した。このレジストパターンをマスクとして、RIEにより磁性層42に達するまでSiO₂膜43をエッチングしてSiO₂膜43に溝45を転写した。このようにして形成された溝領域が記録トラック帯となる。また、レジストパターン下部の磁性層が分離帯として用いられる。

【0133】

次に、図11(b)に表したように、溝領域内にブロックコポリマーを埋め込んで微粒子の規則配列構造を形成した。すなわち、磁性層42の表面をヘキサメチルジシラザンにより疎水化処理した。その後、レジストパターンの残渣をアッシングした。ポリスチレン-ポリブタジエンのブロックコポリマー(PSの分子量Mw=4000、PBの分子量Mw=20000)をトルエンに1%w/wの濃度で溶解した溶液を調製した。

【0134】

基板上に、この溶液をスピンコートしてSiO₂膜43に転写された溝領域内にブロックコポリマー46を埋め込んだ。試料を真空中において150℃で30時間アニールして、ブロックコポリマー46を規則配列化させた。この結果、島状のポリスチレン粒子47が海状のポリブタジエン部分48によって囲まれた構造が形成された。

【0135】

次に、図11(c)に表したように、規則配列した微粒子をマスクとして磁性体ドット49を形成した。すなわち、ブロックコポリマー46をオゾン処理してポリブタジエン部分48を除去した後、水洗した。残ったポリスチレン粒子47をマスクとしてArイオンミリングにより磁性層42をエッチングしてCoCrPtからなる磁性体ドット49を形成した。

【0136】

次に、図11(d)に表したように、RAMビット24間のマトリックスを形成し、表面を平坦化した。すなわち、まず、ポリスチレン粒子の残渣をアッシングした。その後、全面に厚さ約50nmの SiO_2 膜を成膜して磁性体ドット49の間に埋め込んでマトリックス50を形成した。そして、 SiO_2 膜の表面をケミカルメカニカルポリッシング(CMP)により研磨して平坦化した。その後、全面にダイヤモンドライクカーボン(Diamond like carbon)を成膜して保護膜51を形成した。

【0137】

次に、得られた磁気記録媒体表面上で、所定の領域の磁性体ドット49がトラック上に8個配列した部分を認証領域20とし、この部分の磁性体ドット49を全て電子ビーム加熱により、加熱、除去した。

【0138】

この後、この認証領域20に、RAMビットを形成した、すなわち、第1、2、4、5、7、8番目のドット部分に、 $\text{Co}(\text{CO})_8$ 蒸気雰囲気中でガリウムイオン(Ga^+)によるFIB(Focused Ion Beam)スポット加熱を行ったところ、スポット加熱された部分に Co 粒が析出し、磁気情報を記録可能なRAMビット24が形成された。

【0139】

MFM(Magneto-Force Micrography)を用いてこの認証領域を観察したところ、図2に例示したものと同様の配列順序で、磁気的に書き込みが可能なRAMビット24と、バッファ領域と、書き込みができないROMビット26(磁性体ドット49)の存在が確認された。

【0140】

図12に、本実施例の記録媒体を磁気力顕微鏡により観察した結果を模式的に表す。図12に表したように、幅約400nmの記録トラック帯61と幅約40nmの磁性層からなる分離帯62が交互に形成されている。1つの記録トラック帯61内で磁性体ドット49(RAMビット24、ROMビット26)は、マトリックス50によって互いに分離され、六方細密充填構造をなして三角格子を形

成している。磁性体ドット49は、20nm径でトラック方向に沿って30nmのピッチPをもって周期的に形成されてサブトラックを形成しており、記録トラック帯61内には19列のサブトラックが含まれている。

【0141】

このように、磁性体ドット49は三角格子を形成しているため、記録トラック帯61内で隣り合うサブトラック上に位置する最近接の2つの磁性体ドット49はトラック方向に沿う中心間の間隔がサブトラック内のピッチPの1/2だけずれている。

【0142】

次に、図13乃至図15を参照しつつ本実施例の記録媒体を再生する磁気記録再生装置について説明する。

図13は、本実施例の記録媒体および磁気記録再生装置のヘッドスライダを表す断面図である。

【0143】

記録媒体は、ガラス基板41上に磁性体ドット49が規則配列した記録トラック帯61が形成された記録層および保護層51を有する。分離帯62を形成している磁性層には各記録トラック帯のアドレス番号およびセクター番号に相当する情報が予め書き込まれている。

【0144】

ヘッドスライダ70の先端には、読み出しヘッド71と書き込みヘッド72が搭載されている。記録部(RAM)、記憶部(ROM)、信号処理部および制御部は図3と同様に接続されている。ヘッドスライダ70は2段アクチュエータ(図示せず)によって位置決めされる。

【0145】

図14は、ヘッドスライダ70の平面構造を示す概略図である。GMR読み出しヘッド71の寸法は、縦約30nm、幅約20nm、単磁極書き込みヘッド72の寸法は縦20nm、幅約20nmである。

【0146】

図15は、記録トラック帯に対する読み出しヘッドおよび書き込みヘッドの配

置を表す模式図である。但し、読み出しヘッドと書き込みヘッドの距離は、実際の距離を表しているものではない。図15に表したように、記録トラック帯内で所定のピッチで規則配列した19列のサブトラックのうち、2列のサブトラック上の直径20nmの磁性体ドット49を1つの読み出しヘッド71で読み出す。1列のサブトラック上の磁性体ドット49に対して書き込みヘッド82で書き込みを行う。

【0147】

次に、この磁気記録再生装置におけるシーク方法、記録読み出し方法、記録トラッキング方法を説明する。本実施例では、ディスクの外周から所望の記録トラック帯に達するまでの間、横断する記録トラック帯の数をカウントしながら、アクチュエータの加速度および速度を制御する。

【0148】

所望の記録トラック帯に達すると、まず図16に表したように、記録トラック帯の外周側のサブトラック1a上に読み出しヘッド71を設置し、ピッチPに基づく周波数信号のみが検出されるようにトラッキングを行う。得られた再生信号を微分し、記録位置と記録信号を求める。

【0149】

次に、読み出しヘッド71をサブトラック1aと1bの中央に位置するようにアクチュエータを作動する(図15参照)。得られた再生信号と、先に求めたサブトラック1aの信号から、サブトラック1bの信号を演算により求める。この場合、読み出しヘッド71のトラッキングがずれていてもサブトラック1aの信号が前もって分かっているため、サブトラック1bの信号を正確に求めることができる。

【0150】

ここで、図17(a)および図18(a)に例示したように2つのサブトラック上の各磁性体ドット49に所定のデータ信号が記録されており(図17(a)と図18(a)とでデータ信号は同じである)、理想的にトラッキングされている場合(図17(a))とそうでない場合(図18(a))について説明する。

【0151】

読み出しヘッド31は、磁性体ドット49のピッチPの $1/2$ の距離を通過する時間tごとにデータを読み出す。

【0152】

図17(a)に表したように、読み出しヘッド31が2つのサブトラックの中央に正確に位置制御されている場合、図17(b)に表したような実測信号(絶対値)が本実施例の記録媒体に記録される。信号処理部35はこの実測信号を時間tの奇数倍のタイミング(サブトラック1a)および偶数倍のタイミング(サブトラック1b)で分離して、分離された信号強度の絶対値を所定数だけ(例えば3つつ)積分する。

【0153】

図17(a)に表したビットパターンに対して読み出しヘッドの位置制御が正確である場合には、信号強度の積分値の比率は $1:0.8$ となる。磁気記録再生装置の記憶部には、複数の磁性体ドット49への記録状態に応じた様々なビットパターンに対応する信号強度の積分値の理想的にトラッキングしたときの比率が記憶されている。図17(a)の場合には、本実施例の記録媒体に記録された信号強度の積分値の比率と、磁気記録再生装置の記憶部に記憶されている信号強度の積分値の比率とを比較しても差がないので、トラックずれがないと判断できる。

【0154】

一方、図18(a)に表したように、読み出しヘッド31が2つのサブトラックの中央よりサブトラック1a側へずれている場合、図18(b)のような実測信号(絶対値)が記録媒体に記録される。この場合、磁気記録再生装置の信号処理部によって求められる、2つのサブトラック1aおよび1bにおけるそれぞれの信号強度の積分値の比率は例えば $1:0.47$ になる。そして、信号処理部によって記録媒体に記録された信号強度の積分値の比率と記憶部34に記憶されている信号強度の積分値の理想的な比率とを比較することにより、読み出しヘッド31がサブトラック1a側へずれているというトラックずれ情報が得られる。

【0155】

以上のような適切な信号処理により、2つのサブトラックから読み出される信

号強度の積分値の比率を求め、それを記憶部に記憶された積分値の理想的な比率と比較することにより、読み出しヘッドのトラックずれ情報を求めることができる。そして、トラックずれを修正するための動作信号をトラッキング調節用のアクチュエータに送ることにより、正確なトラッキングを実現できる。上記の信号処理および制御は、磁気記録再生装置に設けられた専用のマイクロプロセッサを用いて行われる。

【 0 1 5 6 】

以上のように2列のサブトラックから得られる記録情報を利用して連続的なトラッキングが可能であるが、動作信号の周波数はアクチュエータの微小動作が可能な周波数以下にする。したがって、アクチュエータは微小動作の高周波数対応が可能であることが望ましく、piezo素子を微動アクチュエータに用いた2段アクチュエータが好ましい。

【 0 1 5 7 】

なお、以上では連続する記録ビットから読み出される信号強度を積分する方法を説明したが、記録ビットを例えば10個おきにサンプリングして積分する方法を採用してもよい。

【 0 1 5 8 】

以上、図17および図18を参照して説明したように、磁気記録再生装置の信号処理部は、実際に測定されたサブトラック1aおよびサブトラック1bの信号強度の積分値の比率と、トラッキングが正確に行われている場合のサブトラック1aおよびサブトラック1bの信号強度の積分値の比率（この比率は記憶部に記憶されている）を比較することにより、トラッキング信号を生成する。トラッキング信号は10kHzの周波数でpiezoアクチュエータに送られる。

【 0 1 5 9 】

本実施例において用いる磁気記録装置では、書き込みヘッドの前方に読み出しヘッドが位置し、読み出しヘッドによる検出信号に応じて以下のように書き込みの制御が行われる。トラック方向に沿って規則配列した磁性体ドット49間の間隔とヘッドの走行スピードから、読み出しヘッドによる検出信号が現れると想定される標準的な時間間隔Tが決定される。標準的な時間間隔Tと、実際に読み出

しヘッドにより出力される信号の時間間隔とが制御器により比較される。

【0160】

読み出しヘッドが規則配列領域上を走行している間は、記録ビットから標準的な時間間隔 T に近いほぼ一定の時間間隔で規則的に信号が出力される。なお、実際に信号が出力される時間間隔が、標準的な時間間隔 T に対してしきい値（例えばプラスマイナス 30%）以内であれば、磁性体ドット 49 が規則配列していると判定するようにしてもよい。この場合、読み出しヘッドによる信号の検出時を基準として、所定のタイミングで制御器から書き込みヘッドへ書き込み信号が送られ、書き込みヘッドにより規則配列領域への書き込みが行われる。

【0161】

しかし、読み出しヘッドが欠陥領域上を走行するようになると、磁性体ドット 49 から読み出される信号の時間間隔は、標準的な時間間隔 T と比較してしきい値（例えば、プラスマイナス 30%）を超えてずれるため、磁性体ドット 49 の配列が乱れていると判定される。

この場合、制御器から書き込みヘッドへの書き込み信号が停止され、欠陥領域への書き込みは行われない。

【0162】

読み出しヘッドが次の規則配列領域を走行するようになると、磁性体ドット 49 が規則配列していると判定される。この場合、読み出しヘッドによる信号の検出時を基準として、所定のタイミングで制御器から書き込みヘッドへ書き込み信号が送られ、書き込みヘッドにより次の規則配列領域への書き込みが再開される。

【0163】

なお、磁性体ドット 49 の配列が乱れているか規則的であるかの判定基準は任意に設定できる。例えば、読み出しヘッドからの検出信号の時間間隔の乱れが 3 T 時間以上連続して生じた場合に、磁性体ドット 49 が乱れていると判定するようにしてもよい。

【0164】

また、読み出しヘッドからの検出信号の時間間隔が 3 回連続でしきい値以内の

時間間隔で規則正しい場合に、磁性体ドット49が規則配列していると判定するようにしてもよい。

【0165】

以上、説明したような磁気記録再生装置を用い、本実施例の記録媒体について、前述した第2実施例と同様の手法により、上書きイレースパターン「01010101」を用いたところ、「鍵A」、「鍵B」が取得された。また、この記録媒体をそのままコピーしたRAM磁性媒体では再生不可能なことが確認できた。

【0166】

(第7の実施例)

次に、本発明の第7の実施例として、通常のCD-R (Compact Disk-Recordable) の記録トラックの最内周よりさらに内側に光リソグラフィー法により光記録可能な相変化RAMビットを設け、この領域を認証領域20とした具体例について説明する。

【0167】

図19は、本実施例の記録媒体を表す模式図である。

【0168】

すなわち、まず、普及しているCD-Rと同様の構造を有するライトワンスディスク (Write Once Disk) のデータ格納領域30より、さらに1mmだけ内周の領域に、レジストを塗布した。そして、このレジスト膜に対して光リソグラフィー法により本発明の鍵を取得するための信号が得られるようなビットパターンを持ったドット形状のホールを作成した。

【0169】

次に、相変化材料In-Sb-Teをスパッタ法によりこの領域に積層し、前述のホールを相変化材料で埋めた。

【0170】

最後に、レジスト膜全体をリフトオフ法により除去した結果、ホール内に積層した相変化材料In-Sb-TeからなるRAMビット24以外は全て除去され、CD-Rディスクの内周部に、認証領域20が得られた。

【0171】

このようにして得られた認証領域 2 0 に、光ヘッドにより、前述した第 1 実施例もしくは第 5 実施例と同様の「鍵 A」のビットデータを記録した。

【 0 1 7 2 】

また、この C D - R の記録領域には、先に設けた「鍵 A」および、別途設定した「鍵 B」を用いて暗号化処理により暗号化した動画ファイル・データを記録した。

【 0 1 7 3 】

以上、具体例を参照しつつ、本発明の実施の形態について説明した。しかし、本発明は、これらの具体例に限定されるものではない。

【 0 1 7 4 】

例えば、本発明の記録媒体は、図 1 や図 5 に表したディスク状のものに限定されず、カード状、テープ状、フィルム状などの各種の形態のものも包含する。

【 0 1 7 5 】

図 2 0 は、カード状の記録媒体を例示する模式図である。

【 0 1 7 6 】

すなわち、同図の記録媒体 1 0 D は、有機材料などからなるカードの表面に認証領域 2 0 とデータ格納領域 3 0 が設けられている。認証領域 2 0 は、R A M ビットと R O M ビットとが適宜組み合わせられてなる。また、データ格納領域 3 0 は、R A M あるいは R O M 方式によりデータが記録されている。その記録再生方式についても、磁氣的、光学的、光磁気方式などをはじめとした各種の方式を用いることができる。

【 0 1 7 7 】

図 2 1 は、半導体メモリを用いた記録媒体を表す概念図である。

【 0 1 7 8 】

すなわち、同図の記録媒体 1 0 E は、シリコン (S i) やガリウム砒素 (G a A s) などの半導体を用いて形成された半導体メモリ装置であり、認証領域 2 0 とデータ格納領域 3 0 とが設けられている。認証領域 2 0 は、R A M 型の半導体記憶素子からなる R A M ビットと R O M 型の半導体記憶素子からなる R O M ビットとが適宜組み合わせられてなる。

【0179】

また、データ格納領域30は、RAM型の半導体記憶素子あるいはROM型の半導体記憶素子が集積され、RAM方式またはROM方式によりデータが記録されている。RAM型の半導体記憶素子としては、DRAM (Dynamic Random Access Memory)、FRAM (Ferroelectric Random Access Memory)、MRAM (Magnetic Random Access Memory)、E²PROM (Electrically Erasable Programmable ROM) 等を用いることができる。ROM型の半導体記憶素子としては、SRAM (Static Random Access Memory)、マスクROM等を用いることができる。これらの半導体記憶素子を半導体基板上に集積して形成し、それぞれの記憶素子に記憶された情報を上記実施形態と同様にシーケンシャルに読み出して認証等を行うことが可能である。即ち、この記録媒体10Eの記録再生に際しては、まず、認証領域20に設けられたRAMビット及びROMビットのデータを上記実施形態と同様にシーケンシャルに読み出して「鍵A」を取得し、しかる後に、所定のデータにより認証領域20を上書きイレースする。その後、認証領域20をスキャンすることより、「鍵B」を取得する。

【0180】

そして、これら「鍵A」と「鍵B」に基づいて、データ格納領域30へのアクセスあるいは暗号解読などの可否を管理することができる。

【0181】

【発明の効果】

以上説明したように、本発明によれば、各種の情報を記録した記録媒体において、RAMビットとROMビットとを適宜配置することにより、アクセス制限機能や、コピープロテクト機能や、コンテンツ参照回数制限機能や、コンテンツ閲覧部位管理機能などを、确实且つ容易に与えることが可能となり、デジタルデータの保護に多大に寄与し、産業上のメリットは多大である。

【図面の簡単な説明】

【図1】

本発明の実施の形態にかかる記録媒体の一例を表す模式図である。

【図2】

本発明による認証方法を説明する概念図である。

【図 3】

オリジナル媒体とコピー媒体の違いを表す概念図である。

【図 4】

HDDのようなシステムにおける認証プロセスを例示する概念図である。

【図 5】

複数の認証領域を有する記録媒体を例示する概念図である。

【図 6】

復元処理の応用例を表す模式図である。

【図 7】

本発明の実施例における記録媒体の製造方法を表す工程断面図である。

【図 8】

本発明の実施例の相変化光記録媒体を近接場光顕微鏡により観察した結果を模式的に表す図である。

【図 9】

本発明の実施例の記録媒体の記録再生が可能な相変化光記録再生装置の要部を表す概念図である。

【図 1 0】

本発明の実施例の記録媒体の記録再生が可能な相変化光記録再生装置のヘッドスライダの平面構造を表す概念図である。

【図 1 1】

本発明の実施例の記録媒体の製造方法を模式的に表す工程断面図である。

【図 1 2】

本発明の実施例の記録媒体を磁気力顕微鏡により観察した結果を模式的に表す

【図 1 3】

本発明の実施例の記録媒体および磁気記録再生装置のヘッドスライダを表す断面図である。

【図 1 4】

ヘッドスライダ 7 0 の平面構造を示す概略図である。

【図 1 5】

記録トラック帯に対する読み出しヘッドおよび書き込みヘッドの配置を表す模式図である。

【図 1 6】

記録トラック帯の外周側のサブトラック 1 a 上に読み出しヘッド 7 1 を設置し、ピッチ P に基づく周波数信号のみが検出されるようにトラッキングを行う様子を表す模式図である。

【図 1 7】

理想的にトラッキングされている場合を表す模式図である。

【図 1 8】

トラッキングがずれている場合を表す模式図である。

【図 1 9】

本発明の実施例の記録媒体を表す模式図である。

【図 2 0】

本発明のカード状の記録媒体を例示する模式図である。

【図 2 1】

半導体メモリを用いた記録媒体を表す概念図である。

【符号の説明】

1 0 A ~ 1 0 E 記録媒体

2 0 認証領域

2 2 非記録領域

2 4、2 4 A、2 4 B RAMビット

2 6 ROMビット

3 0 データ格納領域

3 1 ヘッド

3 4 記憶部

3 5 信号処理部

4 1 ガラスディスク基板

- 4 2 磁性層
- 4 4 レジスト
- 4 5 溝
- 4 6 ブロックコポリマー
- 4 7 ポリスチレン粒子
- 4 8 ポリブタジエン部分
- 4 9 磁性体ドット
- 5 0 マトリックス
- 5 0 n m 約
- 5 1 保護層
- 5 1 保護膜
- 6 1 記録トラック帯
- 6 2 分離帯
- 7 0 ヘッドスライダ
- 7 1 ヘッド
- 7 2 ヘッド
- 8 2 ヘッド
- 1 1 1 ガラスディスク基板
- 1 1 2 反射膜
- 1 1 5 溝
- 1 1 6 ブロックコポリマー
- 1 1 7 ポリメタクリレート粒子
- 1 1 8 ポリスチレン部分
- 1 2 0 孔
- 1 2 2 保護層
- 1 3 1 記録トラック帯
- 1 3 2 分離帯
- 1 4 1 記録媒体
- 1 4 2 スピンドルモーター

143 ヘッドスライダ

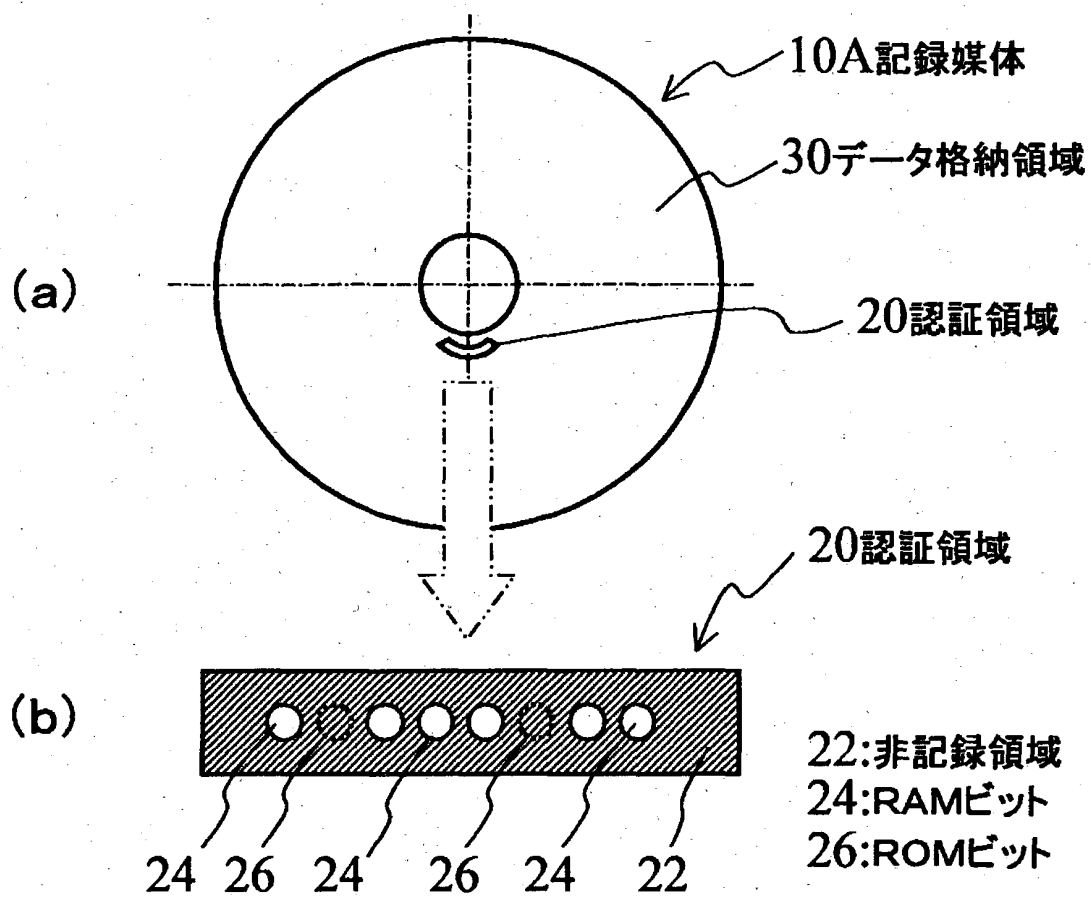
144 ヘッド

145 ヘッド

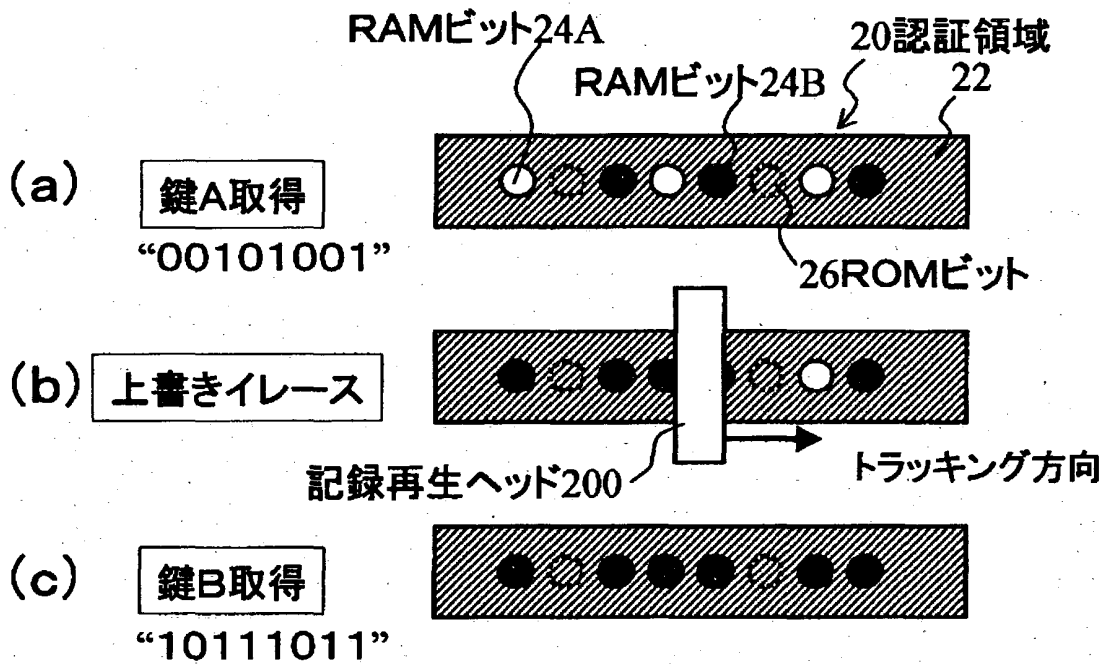
200 記録再生ヘッド

【書類名】 図面

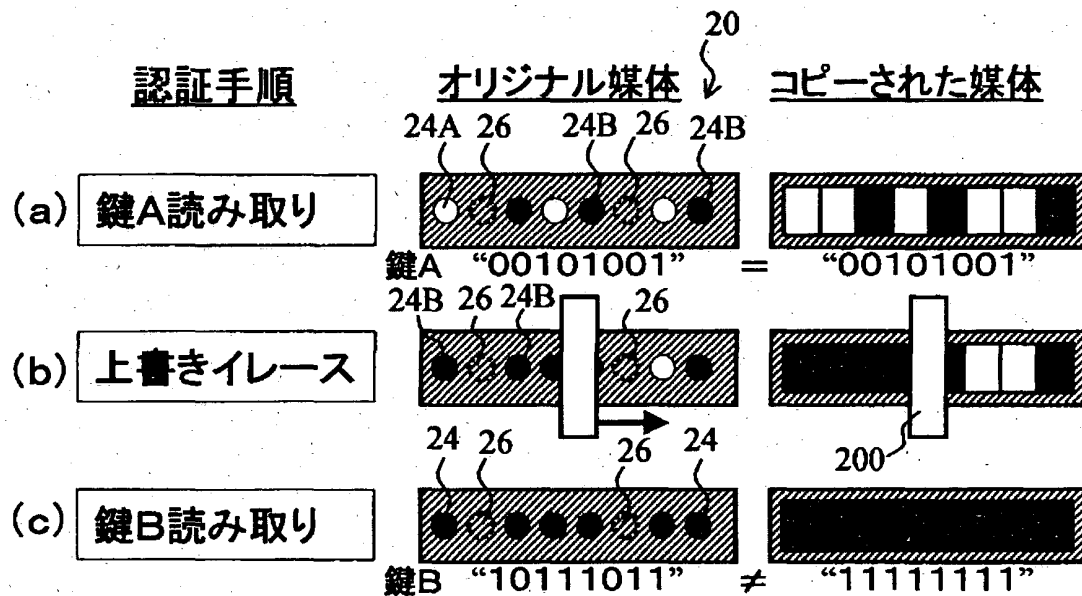
【図1】



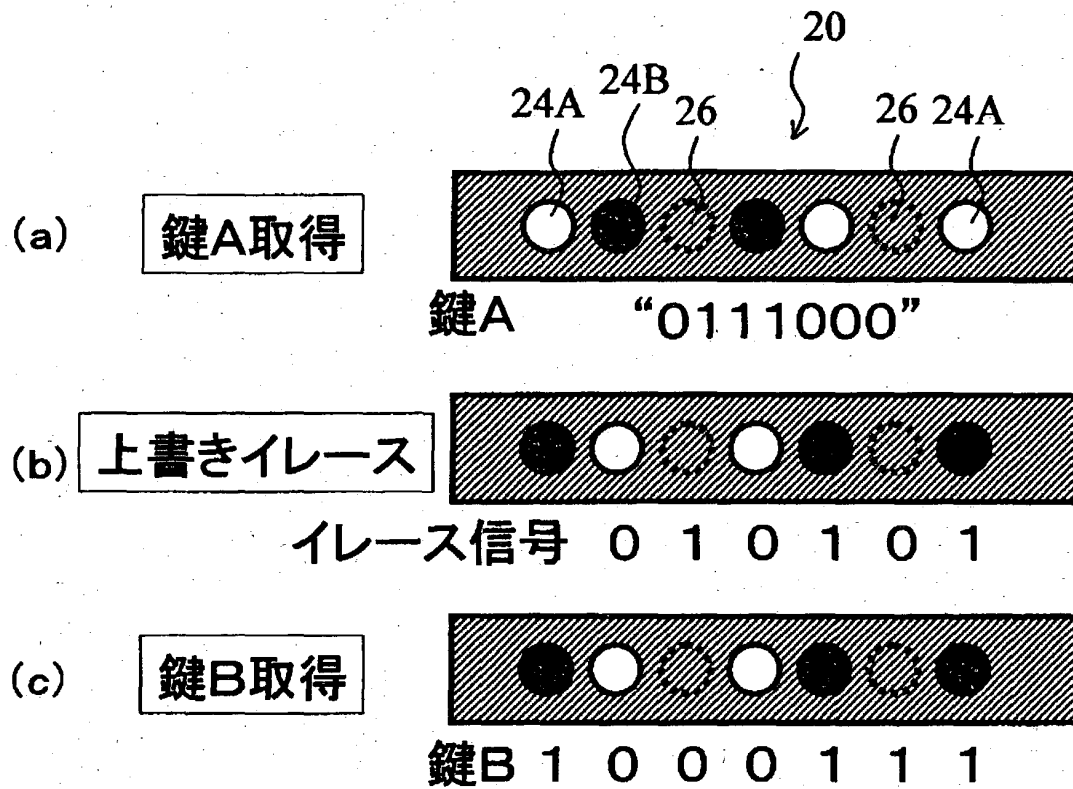
【図2】



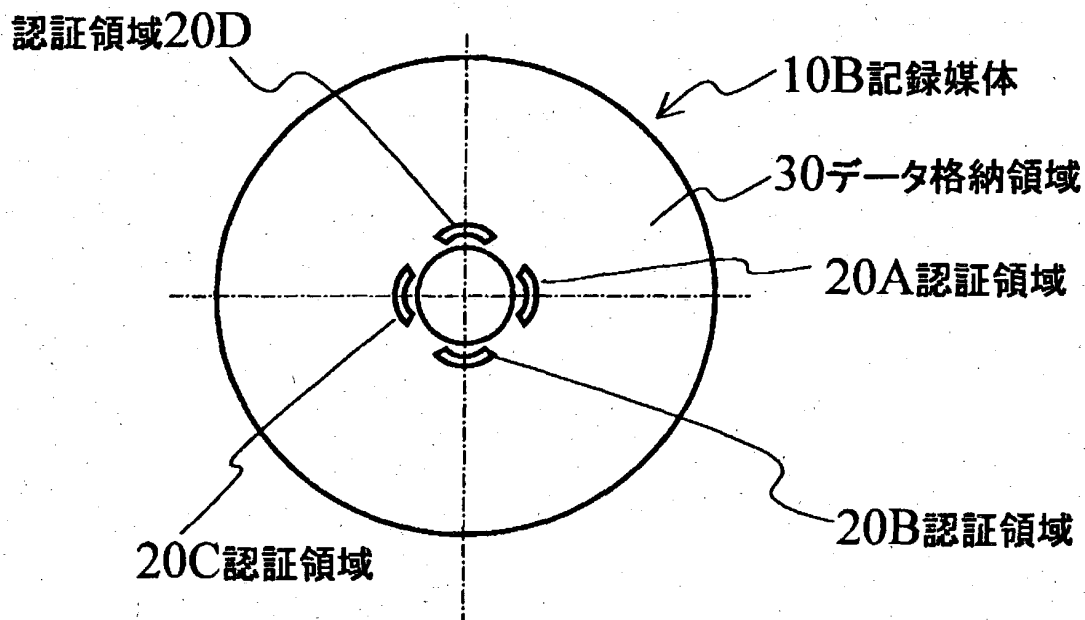
【図3】



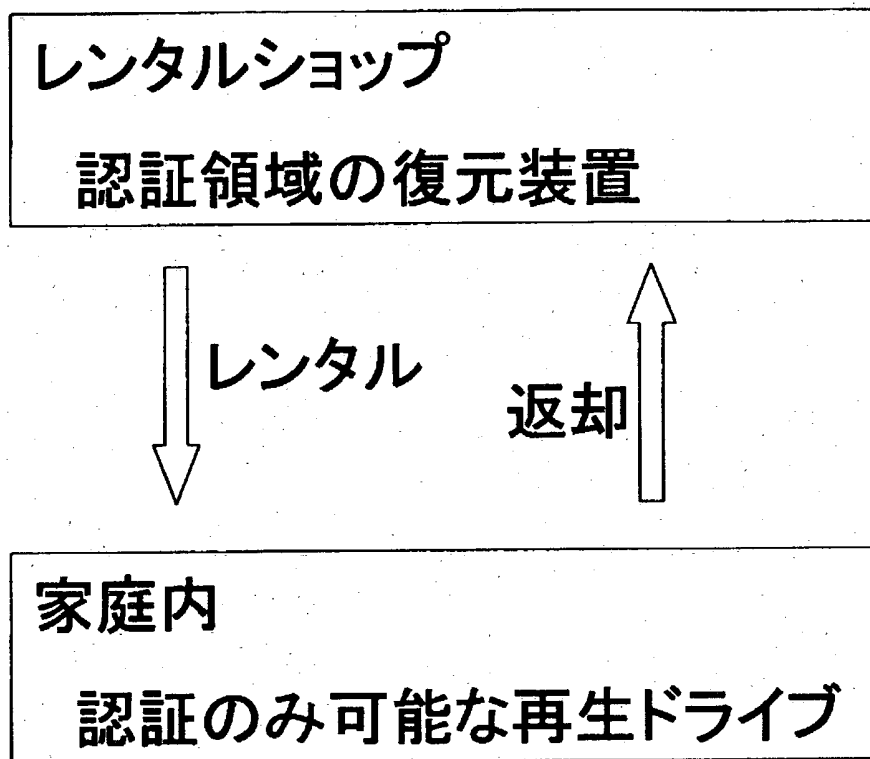
【図4】



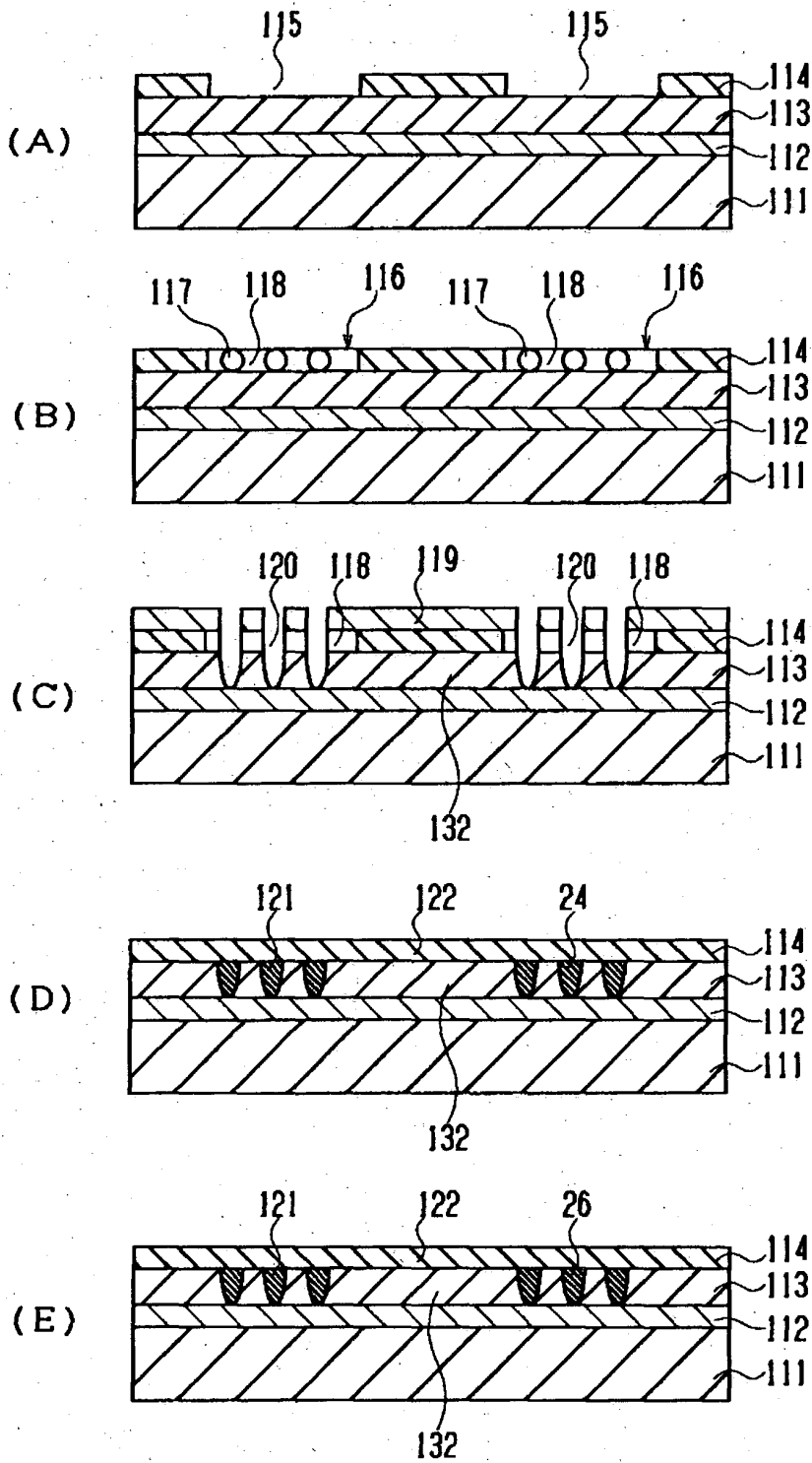
【図5】



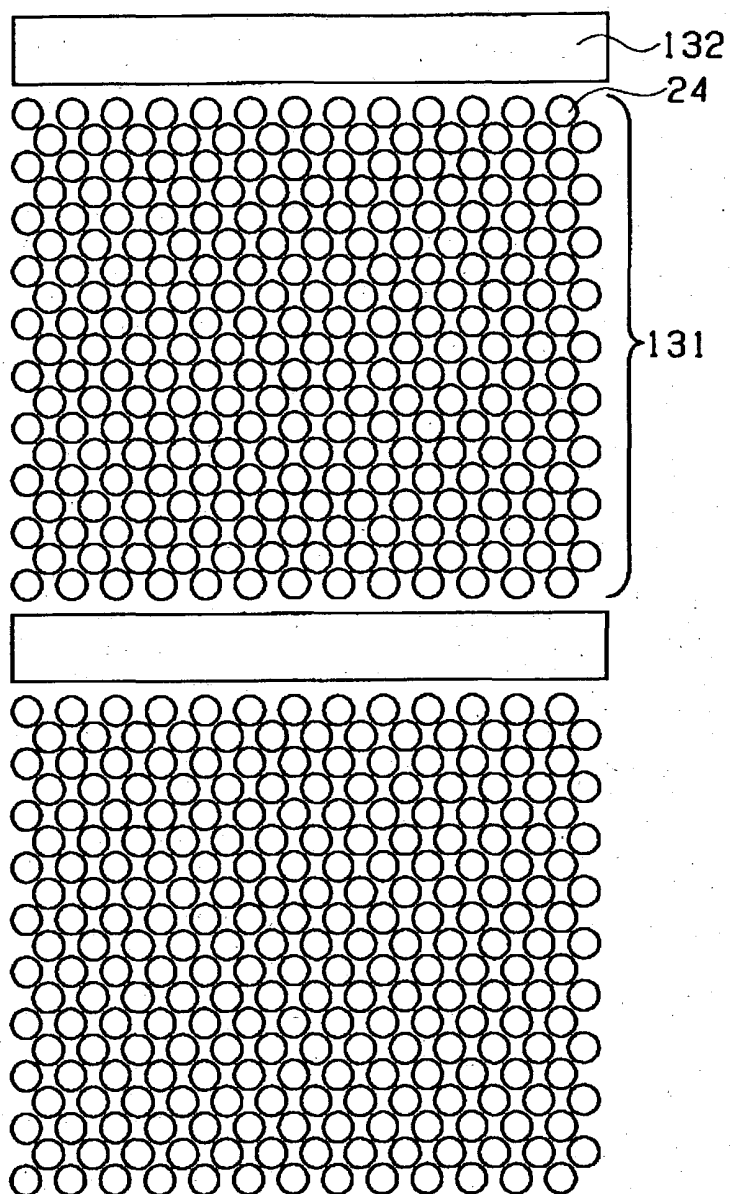
【図6】



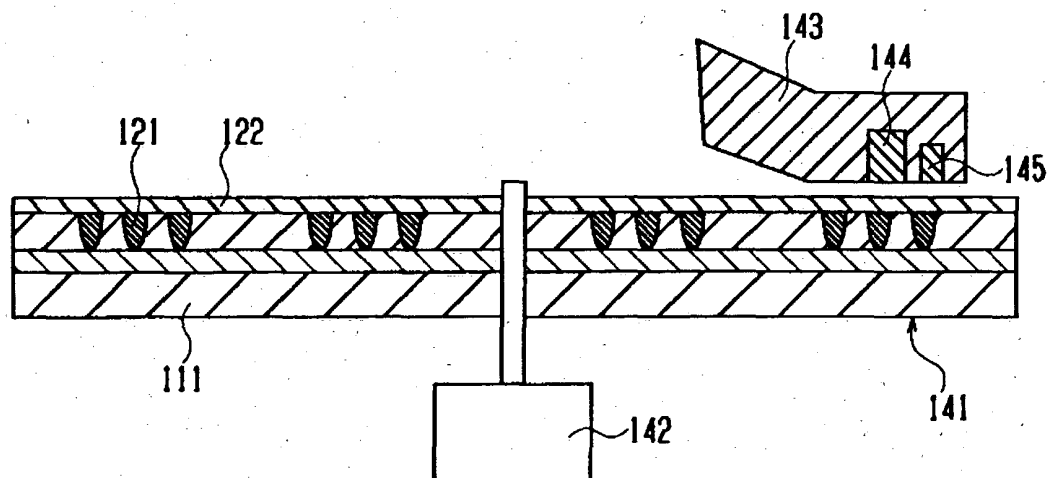
【図7】



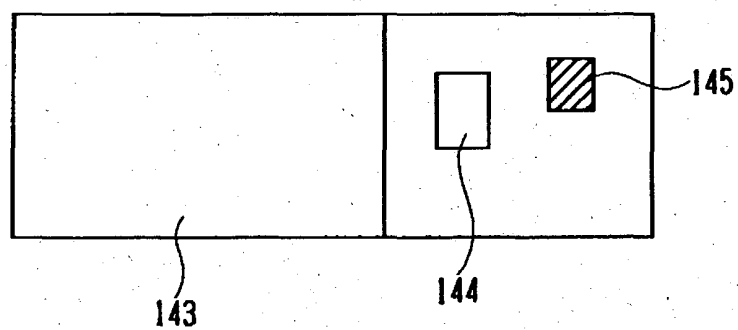
【図8】



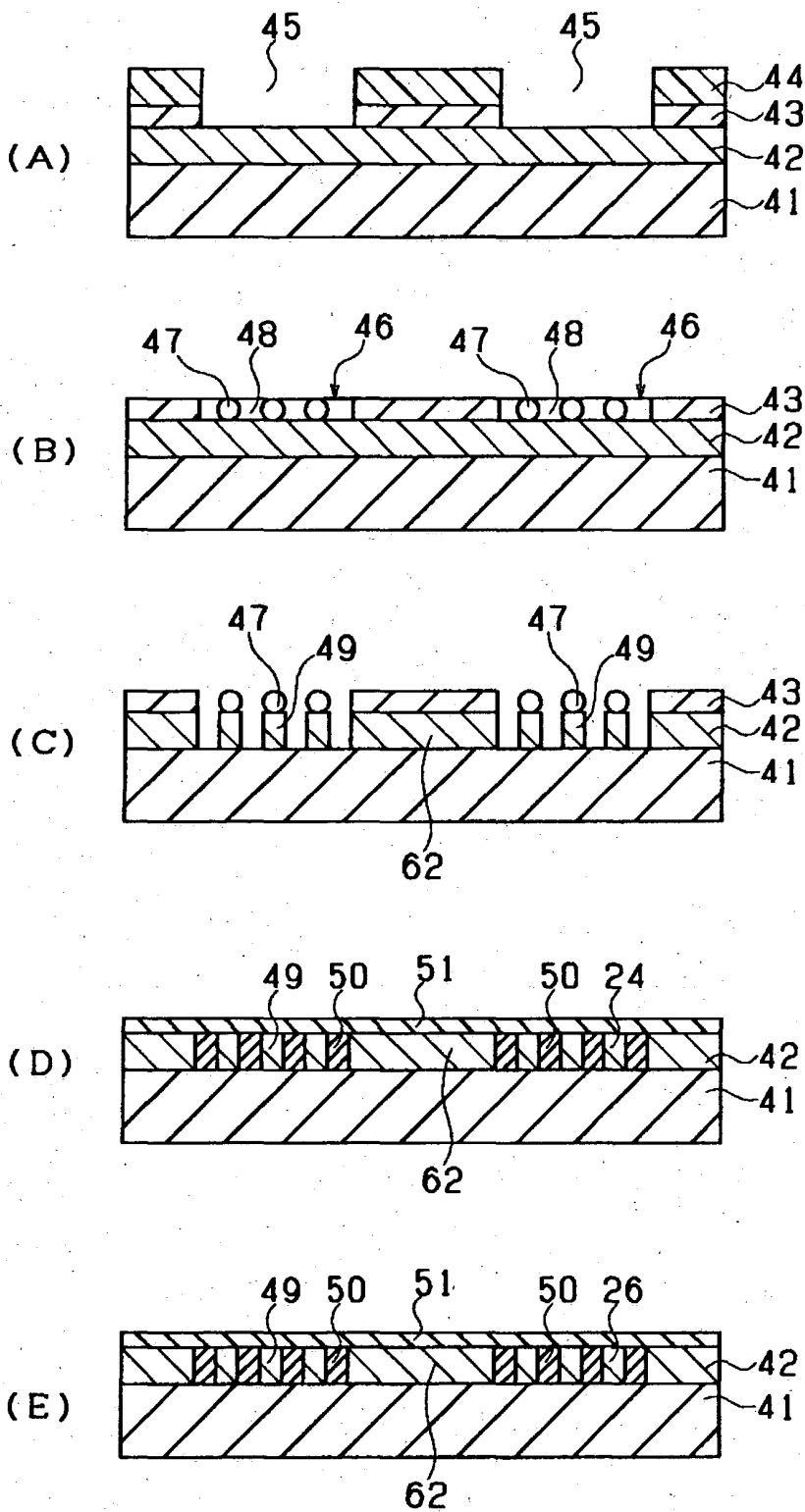
【図9】



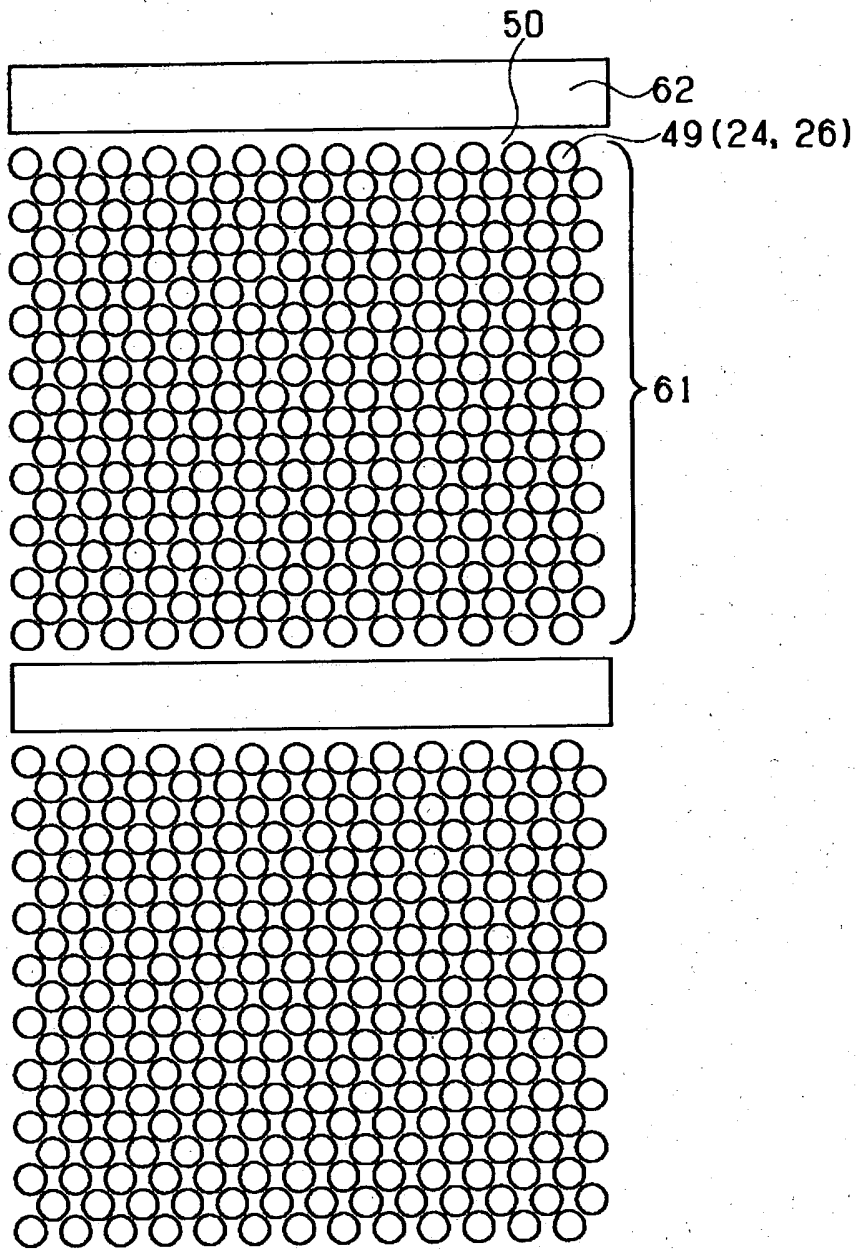
【図10】



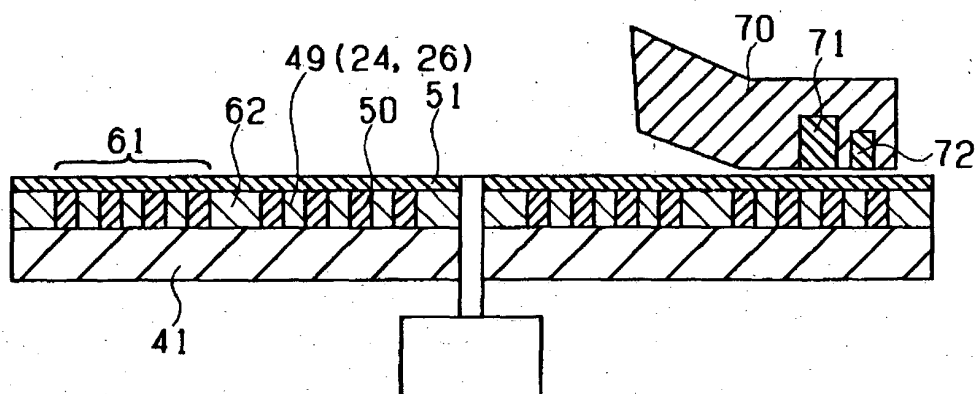
【図 11】



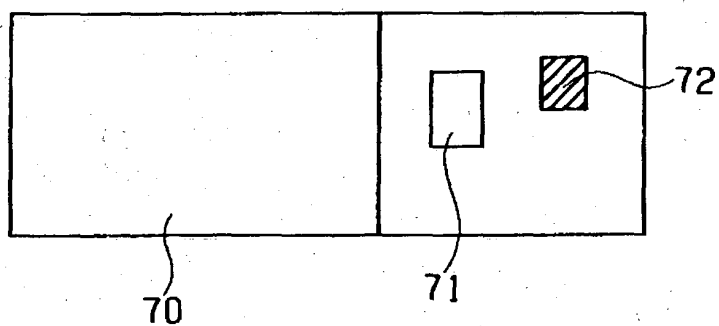
【図 12】



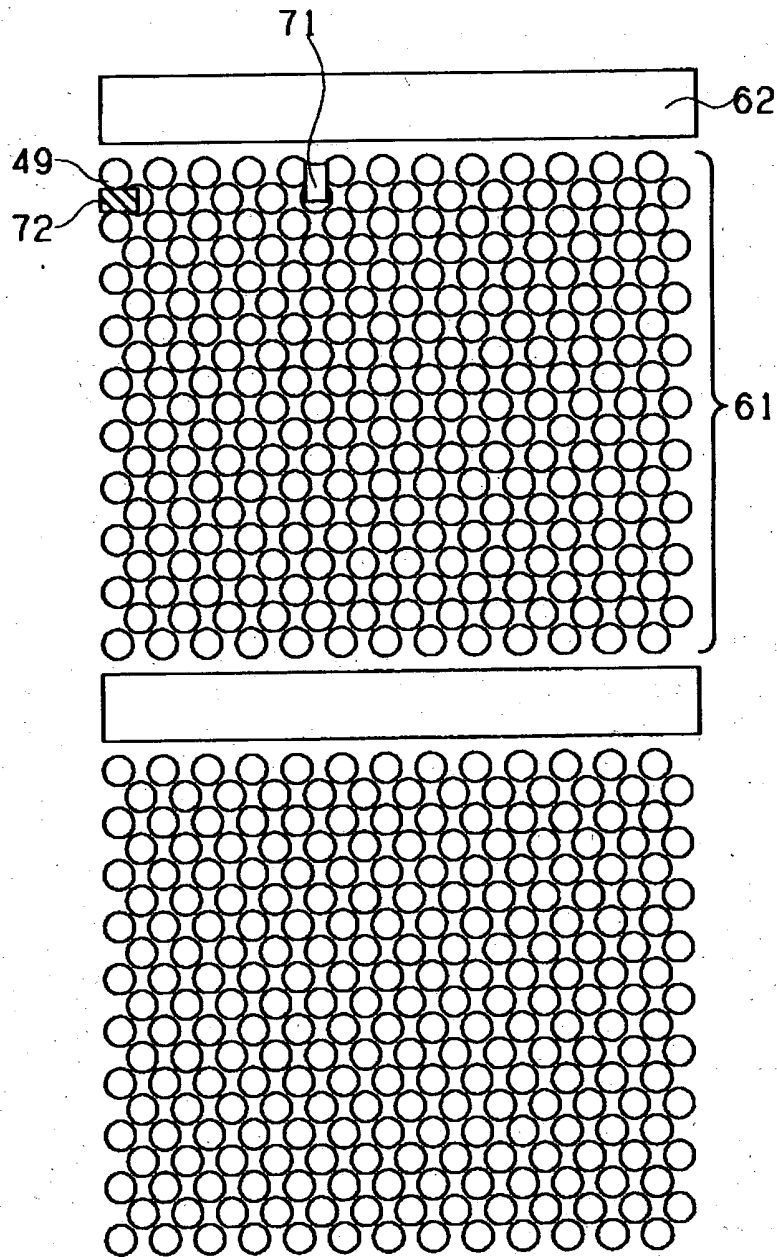
【図13】



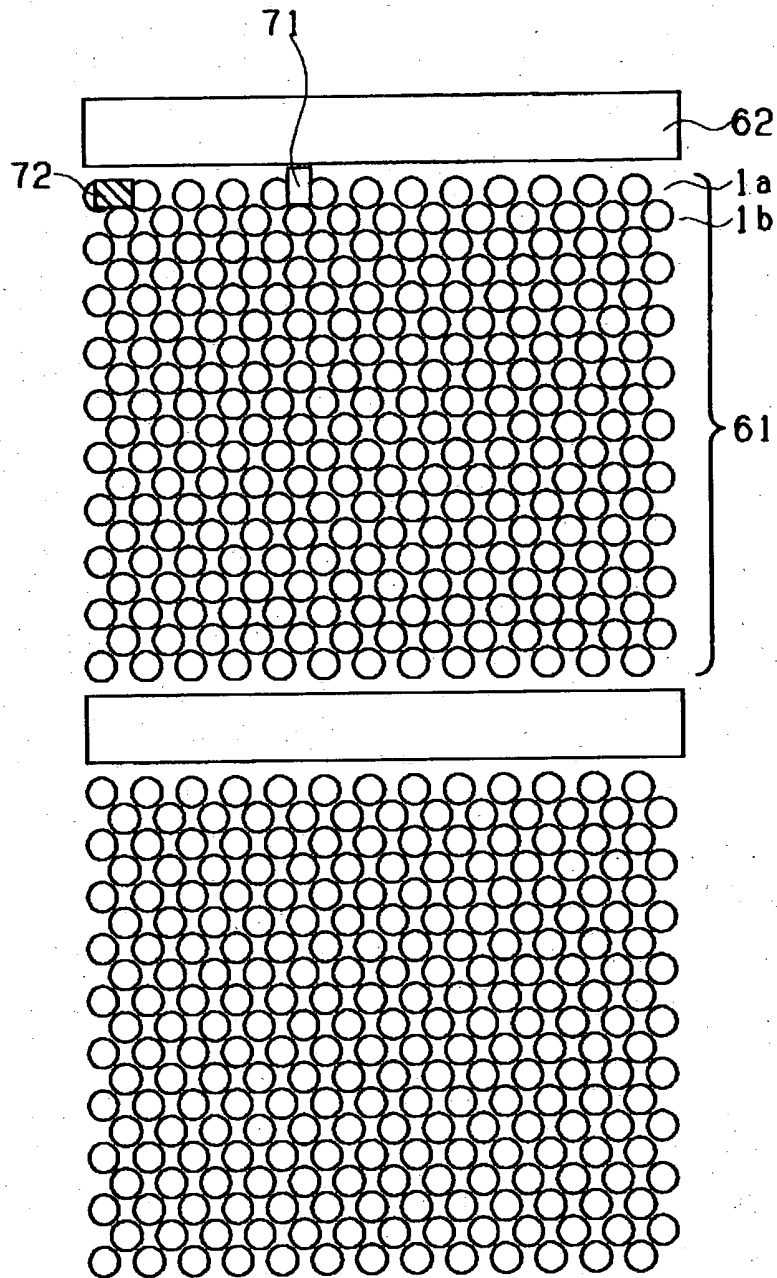
【図14】



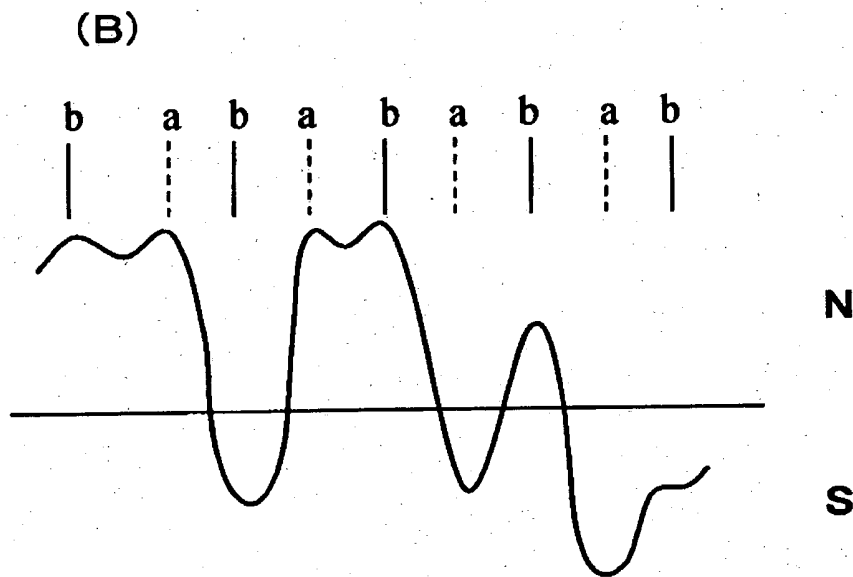
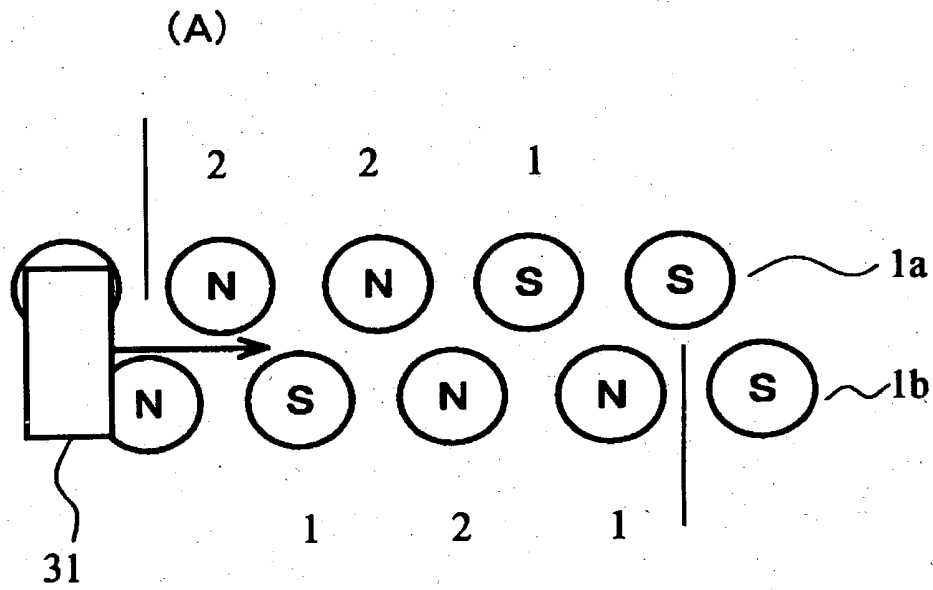
【図15】



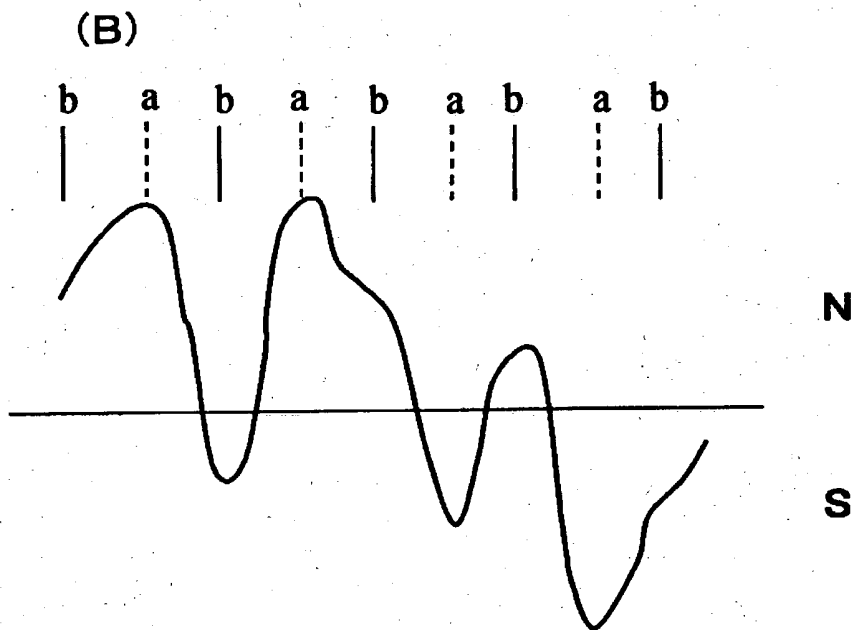
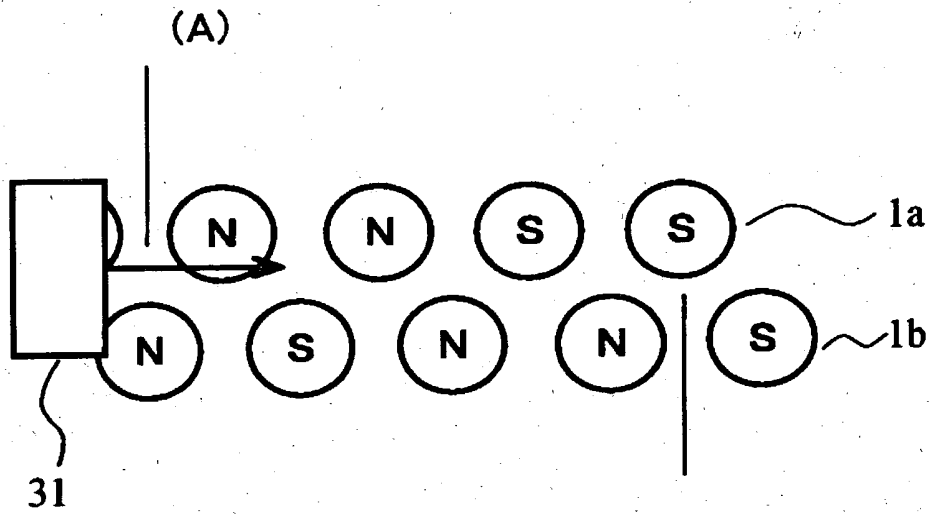
【図16】



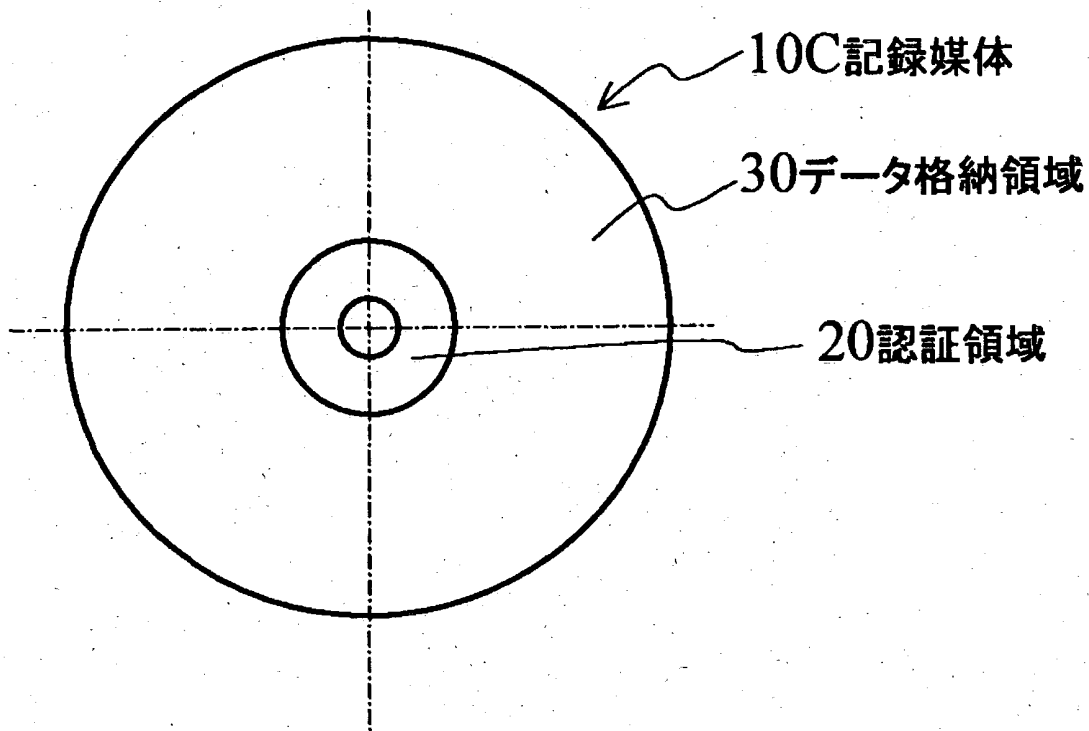
【図17】



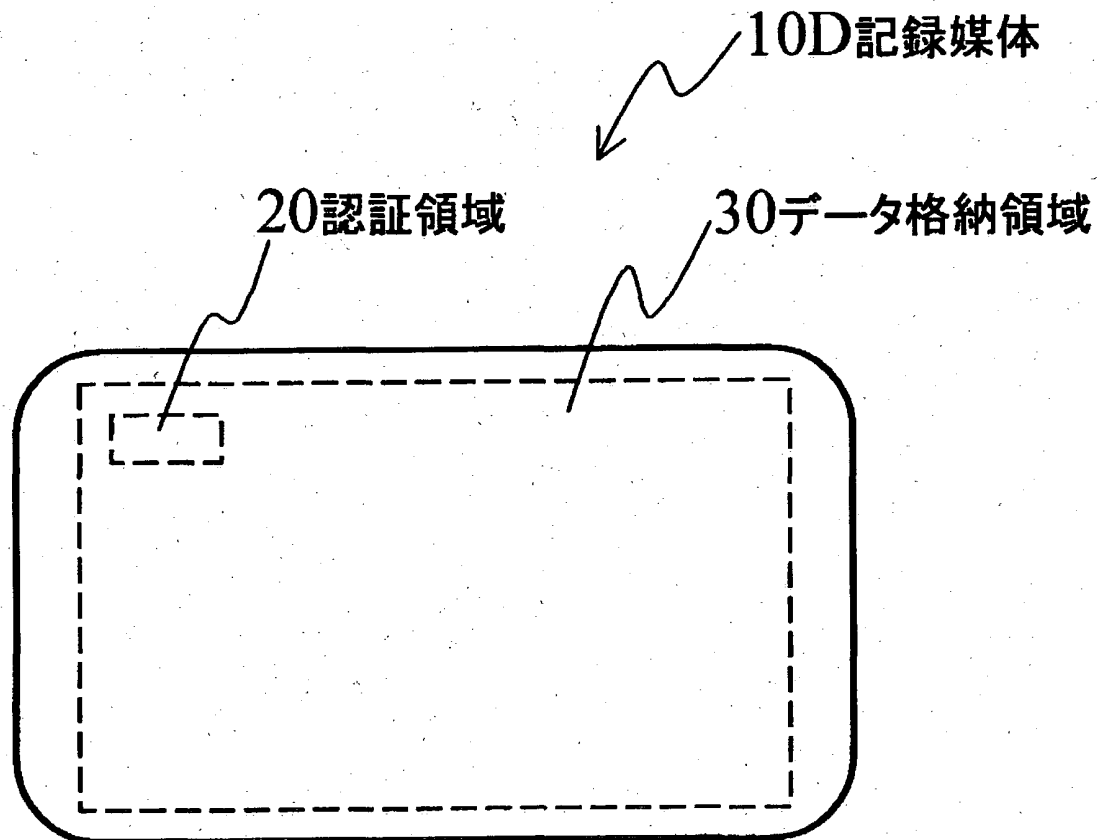
【図18】



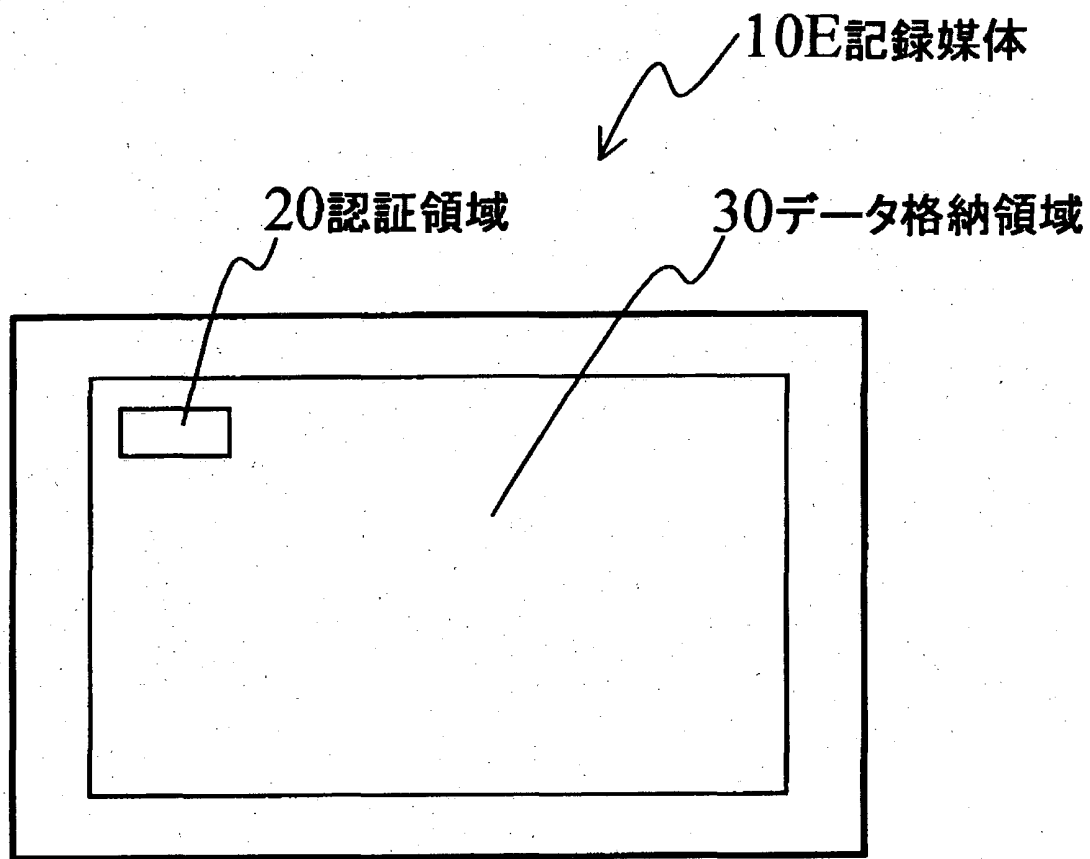
【図19】



【図20】



【図21】



【書類名】 要約書

【要約】

【課題】 記録データに対する安全かつ確実なコピープロテクトを行うことができ、不正コピーを防止できる記録媒体、認証方法、認証システム及び復元システムを提供することを目的とする。

【解決手段】 RAMビット（24）とROMビット（26）とが配列してなる認証領域（20）におけるRAMビット及びROMビットのデータを読み出してその配列に基づいた第1のデータ列（鍵A）を取得し、RAMビットに任意のデータを上書きイレースし、RAMビット及びROMビットのデータを読み出してその配列に基づいた第2のデータ列（鍵B）を取得し、暗号化されたデータの復号化処理を、前記第1及び第2のデータ列に基づいて実行する認証方法を提供する。

【選択図】 図2

出願人履歴情報

識別番号 [000003078]

1. 変更年月日 2001年 7月 2日

[変更理由] 住所変更

住 所 東京都港区芝浦一丁目1番1号

氏 名 株式会社東芝